MALICIOUS HACKERS:

A FRAMEWORK FOR ANALYSIS

AND CASE STUDY

THESIS

Laura J. Kleen, Captain, USAF

AFIT/GOR/ENS/01M-09

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U. S. Government.

AFIT/GOR/ENS/01M-09

MALICIOUS HACKERS:

A FRAMEWORK FOR ANALYSIS AND CASE STUDY

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Laura J. Kleen, M.S.

Captain, USAF

March 2001

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GOR/ENS/01M-09

MALICIOUS HACKERS:

A FRAMEWORK FOR ANALYSIS AND CASE STUDY

Laura J. Kleen, M.S.

Captain, USAF

Approved:

15 March 01
date

Richard F. Deckro, DBA (Advisor)
Professor of Operations Research
Department of Operational Sciences

28 FEB 01
date

Michael G. Morris, PhD, Major, USAF
Assistant Professor of Information Resource Management
Department of Systems and Engineering Management

ACKNOWLEDGEMENTS

> "What you are, stands over you the while, and thunders so that I cannot hear what you say to the contrary." --- *Emerson*

I would like to express my most sincere thanks to several of the people who have stood by me during the long, and often dreary, thesis process. First, I acknowledge the support and encouragement of the ENS department. I would like to especially thank my advisor Dr. Deckro, who helped make sense of an ever-expanding topic area. I also owe thanks to my reader, Major Morris, who took the time to share his expertise with a student from a different department. In addition to the faculty, the assistance of numerous experts was required to give this work a true basis in the world of Information Operations and computer security. I owe you many thanks. Finally, thank you to my soon to be husband, "Blotto" – you carried my backpack when my back was broken and carried my confidence when there seemed too much work to ever bring to closure.

Laura J. Kleen

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF EQUATIONS

AFIT/GOR/ENS/01M-09

ABSTRACT

Recent years have seen an increase in the number and severity of Information Operations (IO) attacks upon DoD resources. At a higher level, the US as a whole has come under cyber attack by individuals and groups seeking thrills, monetary gain, publicity for their causes, and myriad other goals. This effort develops a first cut model of individual hacker mentality that can be utilized to improve threat assessment, mitigate Information Assurance (IA) vulnerabilities, and improve risk assessment. Further, it is a first step toward automated characterization of Information Warfare (IW) attacks based upon hacker types.

All hackers are not the same. In order to best deal with their actions and the intent behind their actions, one must understand who they are. Many hackers are not malicious, in that they hack for the thrill of learning and to "look around". However, others are intent upon gathering information for gain (profit or intelligence aspects), corrupting data or denying access to the system, or to see what harm they can cause. Research for this effort specifically focused on malicious hackers working for nation states, although the basic framework presented applies in part to any type of hacker. This results in advances in the way that hackers are classified and profiled, with a better understanding of their values, skills, and approaches to hacking. Responses can then be tailored to specifics of a given class of hackers. The model developed is illustrated by a case study.

MALICIOUS HACKERS:

A FRAMEWORK FOR ANALYSIS AND CASE STUDY

1. Introduction

1.1. Background

Recent years have shown an increase in the number and severity of computer network incidents on Department of Defense (DoD) resources. The threat that individuals and groups will launch a successful computer based, asymmetric attack against DoD resources is real. At a higher level, the United States (US) as a whole has come under cyber attack by individuals and groups seeking thrills, monetary gain, publicity for their causes, and a myriad of other goals. Figure 1-1 shows the growing trend in computer security incidents being reported to the Computer Emergency Response Team (CERT). This research effort develops a model of individual hacker mentality, focusing on average members of foreign government IO groups, that can be utilized to improve threat assessment, mitigate Information Assurance (IA) vulnerabilities, and improve risk assessment for the DoD, other US government agencies, and US-based corporations. Further, it is a first step toward automated characterization of Information Operations (IO) and Information Warfare (IW) attacks based upon hacker types.

The Air Force defines Information Operations (IO) as those operations that are conducted to defend one's own, or attack an enemy's, information or information systems (AFDD 2-5, 1998: i). This concept for IO applies to all military operations from peace up to and including war and the return to peace (AFDD 2-5, 1998: vii). AFDD 2-5 further defines information warfare (IW) as information operations conducted to pursue one's specific objectives against a specific opponent during times of crises or conflict (AFDD 2-5, 1998: 42). Finally, Information Assurance (IA) efforts are activities that defend information and information systems from attack. These activities seek to ensure the availability of the information and information systems, the integrity of the information, authentication of the data and of system users, confidentiality of the data, and provide for non-repudiation (AFDD 2-5, 1998: 41).

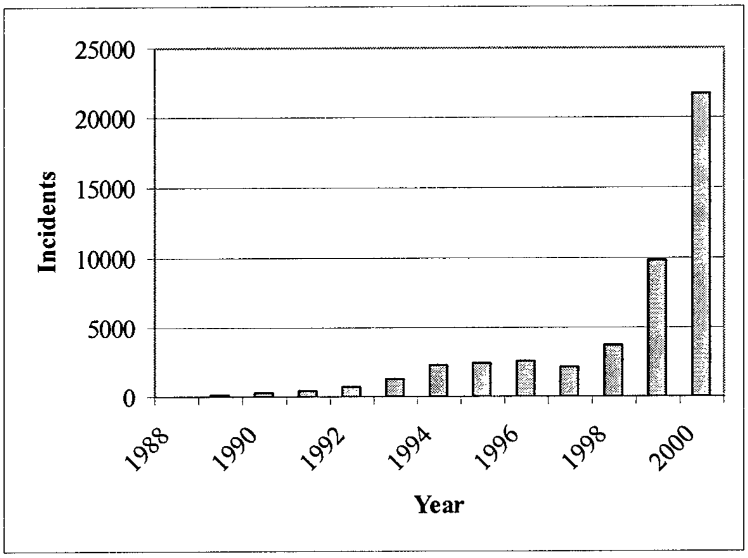


Figure 1-1 US Security Incident Trends (CERT, 2001)

Potential threats to Department of Defense (DoD) systems include foreign and domestic, overt and covert attempts to exploit DoD information and information systems (JP 3-13, 1998: III-6). Domestic threats, those launched from within the United State's borders, present a counterintelligence situation, but are handled as a law enforcement issue in accordance with intelligence oversight regulations (JP 3-13, 1998: III-6). The types of attacks experienced in the US to date include both unstructured and structured attacks (Lemon, 2000).

Unstructured attacks include hackers acting alone or in small groups for individual goals (financial gain, thrills, or both) in traditional categories of novice and expert, malicious and non-malicious (Lemon, 2000). The novice attacks often just copy code easily obtained on the World Wide Web – members of this category are often referred to as "script kiddies". Structured attacks have clear objectives, have financial backing, are organized, and have means in place to support collection of information about the target information or information systems (AFDD 2-5, 1998: 6).

At a more serious level than script kiddies are the structured attacks by transnational and national groups. Some authors describe these groups as Political and Governmental, with Governmental being a higher level of the Political (Vanesevich, 2000) category. Lemon, in a Computer Systems and Networks threat briefing, describes transnational groups as semi-structured, using the phrase "hactivism" (Lemon, 2000). This category includes such activities as efforts by a Muslim interest group, a Tamil Tigers group, the Russian hackers union, and Chinese citizens' efforts following the accidental US bombing of the Chinese embassy during the Kosovo conflict. These groups often launch a cyberprotest using Denial of Service and website hacks with some limited warnings prior to action.

The third, and perhaps most serious, group are the nation states. These are considered "enterprise", or very structured / doctrinal, attacks. Russia has the oldest IO program among nation states (Lemon, 2000). The Russians equate IW on the same level of seriousness as nuclear attacks. The Chinese have even conducted IO efforts as part of their military exercises (Borland, 2000). According to *Newsweek*, as many as 13 countries, including France and Israel, have IO activities directed at the US (Vistica, 2000). Finally, there is the potential for surrogates to be used as a means of IW attack. This could either be groups (transnational or national) hiring "outside" expertise in IO, or groups developing their own attacks and releasing these "tools" on the web for use by script kiddies. It can be very hard to trace these surrogate attacks to the underlying group.

In October 1996, then CIA Director John Deutch called cyberspace attack the third most important threat to national security (Scott, 1996: 60). USAF Lt. Gen. Lincoln D. Faurer expanded this view, saying that the results of a cyberspace attack could equal that of a conventional war. Leadership at all levels of the Department of Defense (DoD) has long recognized the importance of IO and IW. Former USAF Chief of Staff Gen. Ronald Fogleman highlighted the importance of IO concepts in a 1995 speech "Fundamentals of Information Warfare – An Airman's View". Gen. Fogleman stressed that enemies see our computer networks and weapon systems in the same way that we see their computer infrastructure – as key targets in future conflicts (Fogleman, 1995). The widespread and growing integration of information technologies into day-to-day Air Force operations only makes these targets more valuable. The interdependent nature of the military and national information infrastructures could be the weak spot that allows a conventionally inferior enemy to win in a conflict with the United States (AFDD 2-5, 1998: 6). China views this asymmetric impact of IW attack as a key benefit of IW (Farris, 2000: 4).

The Army and Air Force have already begun to raise concerns over the growing DoD dependence upon Commercial-off-the-Shelf (COTS) and Government-off-the-Shelf (GOTS) software in new weapon systems. These software packages are readily available to potential enemies who can then identify the system's inherent security weaknesses (Stevens, 1996: 46). This threat has grown with globalization of software companies. Parts of software code are written in countries throughout the world, with the software companies themselves unsure of the exact nature of all of the lines of code (Lemon, 2000). The rapid growth of the worldwide computer network has exposed parts of our capabilities and weaknesses to the world at large as never before.

News articles reporting incidents of computer break-ins and computer crime are on the rise. The Pentagon itself is currently hacked over 250,000 times a year, with over 500 attacks seen as serious efforts to gain classified information (Vistica, 2000). This number does not include attacks upon the individual services, or worse, those attacks that go unnoticed. Michelle Van Cleave, general counsel to the US Senate Judiciary subcommittee on Technology, Terrorism, and Government Information believes that countries of concern that have a level of computer skill could develop weapons that would wreck havoc on the US if properly used by an adversary (Borland, 2000). At the terrorist level, the Irish Republican Army and Sri Lanka's Tamil Tigers have begun developing a background in IW. 1998 saw the Tamil Tigers using weapons such as e-mail bombs in their attacks against Sri Lanka's government (Borland, 2000).

The cost of these attacks, both in direct economic losses and in costs associated with tracking down those involved, is growing. Estimated losses have grown from $100 million in 1997 to $123.8 million in 1999 (Computer Security Institute, 2000). These amounts are based only on the losses that could be quantified and that were reported; 30% of those companies reporting losses could not determine exact figures for losses of such things as proprietary information or from denial of service.

In order to secure systems against attacks, information system security must focus on several areas. These include confidentiality, protection from computer viruses and other efforts to deny service, protection from alteration or destruction of data, and providing a high level of confidence that data exchanges are only between approved and authorized users (Minihan, 1996: 17). Data encryption, access controls, data authentication, digital signatures, and Internet security protocols are all tools to increase information protection. Another tool is profiling of the potential attackers, which is the focus of this research effort.

1.2. Problem Statement

All hackers are not the same; they differ in skill level, motivations, and methods (Lemon, 2000; Vanesevich, 2000). In order to best deal with their actions and the intent behind their actions, one must understand who they are. A large number of hackers are not malicious, in that they hack into a system for the thrill of learning and to "see what they can see". However, other hackers are intent upon gathering information for gain (profit or intelligence aspects), corrupting data or denying access to the system, or just to see what harm they can cause. For the purpose of this research, the term "hacker" will be used to describe an individual who maliciously, or without authorization, breaks in to a computer system, whether to gain information or exploit the system in some other fashion. Research for this effort was specifically focused on malicious hackers working for nation states, although the basic framework presented would apply in part to any type of hacker. This thesis reviews existing methods and proposes advances in the way that hackers are classified and profiled, with the goal of a better understanding of their values, skills, and approaches to hacking. By understanding the enemy, responses can be tailored to the specifics of a given class of hackers, leading the way to improved automated response (both capability restoration and attack response) and attack characterization, as well as system defense based upon the need to protect specific information from specific adversaries.

1.3. Problem Approach

This effort develops a scripted profile of the behavior of individual computer hackers by descriptive modeling of hacker types. A scripted profile uses set details about hackers, their motivations, and actions as a sort of "checklist" to describe specific individuals or members of groups. The hacker mentality model developed specifically describes this "Political and Governmental" group of hackers (Vanesevich, 2000), based upon behavioral characteristics. It is envisioned that transnational groups and national groups will be sufficiently different that they will warrant separate detailed models, although different cases of each group could be described within that group's framework. Common aspects of the two groups (transnational and national) will be due to the ties of individual hackers to group goals. However, the way that the two groups approach IO and IW may differ. For example, Lemon sees attacks by hackers with ties to a national group to be more doctrinal (Lemon, 2000). This doctrinal approach may translate to different individual motivations and actions as compared to those of a hacker from a less structured group. The end result is a behavioral model for a hacker within a specific type of social (transnational or national) framework.

Data from past documented cases of hacking can be used to explore characteristics of hackers that can be obtained from the evidence they leave behind. Multivariate analysis of substantiated attacks would prove useful in exploring similarities and differences within the hacker culture. Suggested techniques include cluster analysis, discriminant analysis, and canonical correlation (Mardia, 1994). The objective is to find aspects of substantiated attacks that are in common and not in common, with the goal of separating types of hackers by those aspects. While script kiddies may provide the majority of data, it is the structured attacks that are of interest.

The primary basis of the model developed in this thesis will be an Ishikawa (fishbone) diagram from Total Quality Management. This tool provides a clear picture of the key aspects of the profile, and allows for the hierarchy to be developed at any level needed or desired. The Ishikawa diagram has the added benefit of allowing for interrelationships among areas of the model, which can provide additional insight into the individual being profiled. More details of the Ishikawa diagram, and the process by which it is built, are provided in 3.1.

1.4. Research Scope

This thesis approaches the problem of malicious hackers from a military perspective. While the military shares vulnerabilities and concerns with other governmental and commercial sectors, the proposed model framework focuses on some of the aspects of hackers that are unique to the military. For this reason, the proposed model may not address all aspects relevant to these other sectors of society.

While many classifications of hackers have been proposed (as discussed later), this effort specifically focuses on malicious hackers that are actors for foreign governments. The model developed in this research seeks aspects of the behavior and motivations of these actors that will help IA personnel more readily identify events attributable to foreign nations. Data on substantiated attacks, where available, will assist in model validation. A related area, analyzed to a lesser extent, is terrorists and transnational criminals. Other groups of hackers, such as insiders and those not affiliated with other than their peers in the world of hacking, are not addressed.

One specific limitation of this effort is the amount and type of data that is available. According to the Air Force Computer Emergency Response Team (AFCERT), only a small fraction of suspicious connections to the AF networks are attributed to true "incidents" each year. Statistics for 1999 show 71 incidents found among 368 million suspicious connections. This means that the number of attacks that could be attributed to hackers of interest will be limited. In addition, while several efforts have been made to survey hackers, such as that provided by John Vanesevich's AntiOnline article on hacker profiling (Vanesevich, 2000: n.pg) and Taylor's Hackers, care must be exercised in interpreting the results. There is no assurance that the respondents to surveys or interviews are truly hackers, that they are of the skill level professed, or that they are responding in accordance with their true feelings or thoughts. That being said, this research has been conducted within the limits of the available resources.

1.5. Assumptions

The framework utilized in this thesis relies on some basic, key assumptions:

- A threat warning and assessment has already been accomplished for the group of interest;
- Data is available from previous attacks originating in the country of interest.

1.6. Overview and Format

The remainder of this thesis begins in Chapter 2 with a review of relevant references, sorted by topics such as Information Operations, hackers, the general concept of profiling, and proposed models / frameworks. These works supply a scope to the methodologies and concepts that might prove useful in describing malicious hackers employed by nation states. Chapter 3 develops a framework for analyzing foreign governments hackers, developing key aspects such as motivations, intents, skills, and approach. Insight from the references in Chapter 2 will be used to help "feed" the model developed in Chapter 3. Chapter 4 demonstrates and refines the framework developed by way of a case study of the Chinese and their published views of Information Operations and the future of warfare. Finally, Chapter 5 draws conclusions from the framework developed and the case study, and provides recommendations for future efforts.

2. Review of Relevant References

Since this is a relatively new area of research, there is limited relevant prior direct research to reference. Much of the supporting data for the effort will be gleaned from recently published books on Information Security (Anonymous, 1998; Denning, 1999; McClure, 1999), technical reports, and from news articles. The following review intended to serve four main purposes:

- Identify current military views of information operation and information warfare as they apply to state sponsored hackers;
- Identify past efforts to quantify individual hackers and types of hackers;
- Provide appropriate background information in criminal profiling, motivation and behavioral theory, and multivariate analysis of data; and,
- Provide appropriate background information required to develop a scripted profile of state-sponsored hackers.

2.1. Information Operations

There are many available policy documents and studies that address how the nature of war is changing with the advent of widespread computer technology. Those with the most bearing on this effort are discussed in this section. A key concept, expressed in the Air Force Doctrine Documents (AFDD), is that doctrine must be "alive", it must change with the times if it is to be effective (AFDD 2-1.5, 1998: v). AFDD 2-1.5 suggests that, as technology changes, "new concepts, systems, and procedures" must be developed (AFDD 2-1.5, 1998: 2). With the rapidly evolving nature of IW, those seeking to define their own doctrine, or to understand a potential adversary's doctrine, must at least keep pace with the times, if not "move out in front" to set the pace.

2.1.1. Joint Publications (JP) 3-13

The Joint Chiefs of Staff have provided overall, authoritative guidance for US forces with regard to Information Operations. As mentioned previously, IO "apply across all phases of an operation, throughout the range of military operations, and at every level of war" (JP 3-13, 1998: I-1). It is noted that the boundaries between levels of conflict are more fluid with IO than other types of military operations, providing the chance that effects of IO may be more widespread than was planned, as is shown in Figure 2-1. IW acts, then, are those IO directed during time of war or crisis to achieve specific objectives over a specific enemy. Joint doctrine defines these enemies broadly. An adversary might be a group, organization, or decision maker that could affect the success of joint operations (JP 3-13, 1998: I-1). IW can be used to shape the battlespace and prepare for future operations (JP 3-13, 1998: I-4). However, intelligence preparation of the battlespace is vital to successful IO and IW (JP 3-13, 1998: I-18). This includes efforts such as gathering information on an adversary's information infrastructure and related activities.

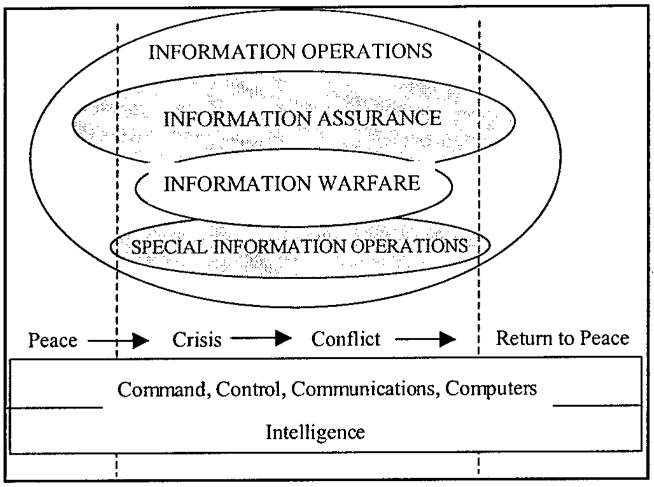


Figure 2-1 IO Relationships Across Time (JP 3-13, 1998: I-4)

At the strategic level of war, IO seek to achieve national objectives by impacting political, military, economic, and informational elements of an adversary's power structure (JP 3-13, 1998: I-2). It also seeks to protect friendly forces from similar attacks by enemy forces. Offensive IO at the strategic level attempts to influence enemy leadership to deter crisis or rapidly end hostilities (JP 3-13, 1998: II-10). Additionally, offensive IO attempts to limit social, economic, and political effects associated with conventional weapons use, speeding recovery once hostilities end (JP 3-13, 1998: II-10). A warning is in order with respect to this concept, since not all countries may be as cautious with regard to synergistic effects. For example, interdependencies in the world financial markets could lead to widespread devastation if an adversary destroyed or degraded key friendly force economies.

Operational level IO supports operations at the campaign or major operation level (JP 3-13, 1998: I-2). Targets include enemy lines of communication, logistics, and command and control. These operations support higher-level goals by degrading the adversary's ability to wage war, while protecting friendly forces information superiority (JP 3-13, 1998: I-3). Offensive IO at the operational level focuses on adversary forces or capabilities in the combatant commanders Area of Responsibility (AOR) (JP 3-13, 1998: II-10). These IO targets may also have strategic value in demonstrating US resolve. In peacetime, offensive and defensive IO at this level may assist in deterrence, assist in operational assessments and estimates, provide situational awareness, and support contingency plans and operations (JP 3-13, 1998: II-10). In crisis and conflict, offensive, operational level IO may help the combatant commander seize and sustain the initiative (JP 3-13, 1998: II-10).

Tactical level objectives for IO involve specific objectives to affect enemy information and information systems that directly relate to the conduct of military operations while protecting friendly force capabilities (JP 3-13, 1998: I-3). At the tactical level, IO may be lead at the joint level, by a single service, or by a component commander. Offensive IO attempts to deny, disrupt, destroy, or otherwise control the enemy's use of and access to information and information systems (JP 3-13, 1998: II-11). The human element is still the focus of operations at the tactical level. Tactical IO attempts to affect the will of the enemy's military forces and general popular support (JP 3-13, 1998: II-11).

Joint doctrine specifically allows for the employment of offensive IO when deemed appropriate (JP 3-13, 1998: I-5). Offensive IO may be used to neutralize adversary capabilities prior to their use against friendly forces, or in response to adversary IO employment (JP 3-13, 1998: III-7). IO may be used in three ways: as a stand-alone operation, a supported operation, or a supporting operation. A stand-alone operation involves IO as the only strategy against the adversary. If IO is the main effort against the adversary, but other capabilities are required, it is a supported operation. Finally, if IO is a force multiplier within a conventional campaign, it is a supporting operation (JP 3-13, 1998: VI-2).

US troops and weapons systems are growing more reliant upon information and information systems. These systems have inherent vulnerabilities as a consequence of enhanced functionality, ease of use, compatibility, and efficiency. For example, the move to Commercial-Off-the-Shelf (COTS) equipment results in cheaper hardware and software, but allows potential adversaries the opportunity to exploit known vulnerabilities in these systems. Additionally, much Department of Defense (DoD) nonclassified information moves over commercial infrastructure, yet the DoD does not have authority to protect the commercial infrastructure it depends on (JP 3-13, 1998: I-12). These commercial systems then become choice targets for potential adversaries. Information and information systems that are integrated, shared, or synchronized during multinational operations present additional key targets to adversaries (JP 3-13, 1998: III-3).

Joint doctrine states that IO is essential to achieving a joint force commander's (JFC) objectives (JP 3-13, 1998: I-3). Additionally, IO "may have their greatest impact as a deterrent in peace and during the initial stages of crisis" (JP 3-13, 1998: I-3). This includes the need for access to information from outside the operational area. The Air Force's Aerospace Expeditionary Force (AEF) relies upon reachback capabilities to limit its in theater footprint. All branches of the military need "frequent, instant, and reliable access to information" to support intelligence efforts and decision making (JP 3-13, 1998: I-15). Doctrine states that information and information systems will be protected relative to the value of information they contain and the risks of compromise or loss of the information (JP 3-13, 1998: I-5).

Several key definitions relating to IO are provided in Table 2-1 IO Terminology.

Table 2-1 IO Terminology

Term	Definition
Computer Network Attack (CNA)	Operations to disrupt, deny, degrade, or destroy information resident in computers or computer networks, or the computers and networks themselves.
Information	Facts, data, or instructions in any medium or form.
Information Assurance	IO that protects and defends information systems. Ensures availability and integrity of data, authentication, confidentiality, and nonrepudiation.
Information-based Processes	Processes that collect, analyze, and disseminate information in any medium or form.
Information Operations (IO)	Actions taken to affect adversary information and information systems, while defending one's own information and information systems.
Offensive IO	IO involving integrated use of capabilities and activities, supported by intelligence, to affect enemy decision makers and achieve specific objectives.
Defensive IO	IO that integrates policies and procedures, operations, personnel, and technology to protect information and information systems.
Information Superiority	The capability to collect, process, and disseminate information while exploiting or denying that ability to the enemy.
Information System	Infrastructure, organizations, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.
Information Warfare (IW)	IO conducted during time of crisis or war to achieve specific objectives over a specific adversary
	Source: JP 3-13, I-9 – I-11

In order to plan offensive and defensive IO, the nature of a specific threat must be understood. JP 3-13 states that an IO threat should be defined in terms of "a specific adversary's intent, vulnerability, capability, and opportunity to adversely influence the elements of the friendly information environment critical to achieving objectives" (JP 3-

13, 1998: I-16, I-18). It defines an adversary as being organized, supported, and politically sponsored or motivated to affect decision makers (JP 3-13, 1998: I-16). The effects of targeting enemy information and information systems can focus upon a widespread or narrow range of enemy systems and capabilities (JP 3-13, 1998: II-10).

JP 3-13 addresses both offensive and defensive operations. Both depend upon information to plan and conduct operations. However, due to the nature of this research effort, only the offensive side of IO and IW will be discussed. US offensive IO doctrine will be used to provide insight into that of potential adversaries. The grand target of offensive IO is the adversary's human decision making processes (JP 3-13, 1998: II-1). Potential IO targets are presented in Figure 2-2. Offensive IO objectives must be clear, support higher-level objectives, and provide identifiable measures of success (JP 3-13, 1998: II-1). The US limits it employment of offensive IO in some situations. Actions must be appropriate for the specific situation and consistent with stated objectives. Additionally, the actions must be "permissible under the law of armed conflict, consistent with applicable domestic and international law, and in accordance with applicable rules of engagement" (JP 3-13, 1998: II-1). Finally, the value of a target as an exploitable intelligence source must be weighed against the need for its destruction or damage. A target can be isolated, neutralized, or bypassed in order to keep its intelligence value intact while supporting other operational needs for offensive maneuver (JP 3-13, 1998: II-14). To ensure efficient IO attacks, one must:

- Understand the adversary's perspective and how IO may influence it.
- Establish clear IO objectives
- Identify the value, use, and flow of information, and its vulnerability

- Identify specific targets to meet objectives
- Determine target sets
- Determine the best set of capabilities to use against the targets
- Predict consequences of employing specific capabilities at a predetermined level of confidence
- Obtain approval to employ offensive IO
- Identify support necessary to support assessment
- Integrate, coordinate, and implement IO
- Evaluate outcomes (JP 3-13, 1998: II-1 –II-2).

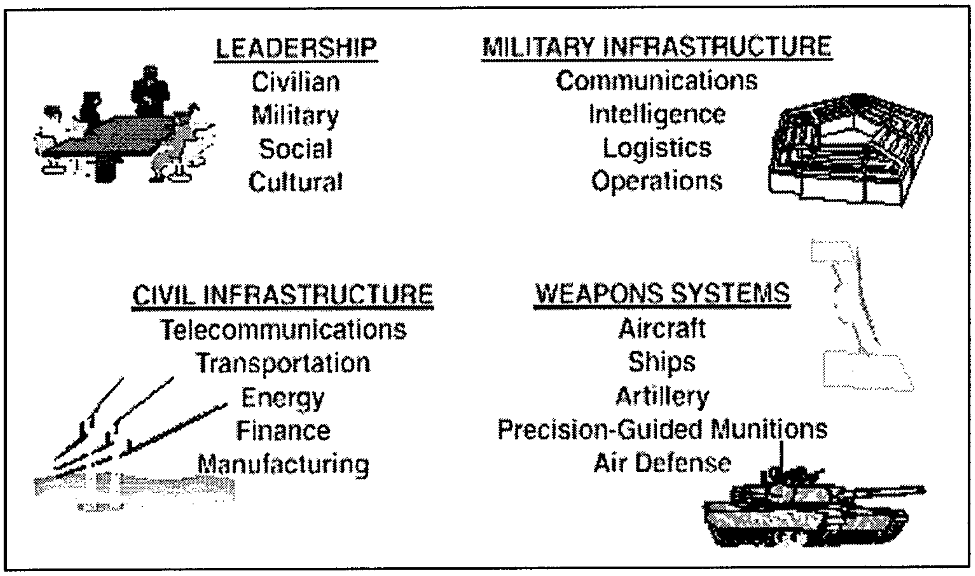


Figure 2-2 Examples of Potential IO Targets (JP 3-13, 1998: I-17)

Military operations or capabilities such as electronic attack (EW) and physical attack / destruction may be combined with IO to produce a synergistic effect (JP 3-13, 1998: II-3). Six of these key capabilities, as they apply to IO, are summarized in

Table 2-2 Key Military Capabilities.

Offensive IO can be used in peacetime with approval of the National Command Authority (NCA). In these cases, IO is used to support peace, as a deterrent or power projection, and to control escalation of hostilities (JP 3-13, 1998: II-8). Offensive IO may also be used during Military Operation Other than War (MOOTW) not involving the threat or use of force. IO would seek to affect adversary Courses of Action (COA) or degrade the adversary's ability to respond. In this case, IO supports objectives of maintaining or returning to peace (JP 3-13, 1998: II-8). IO could also be used to prepare the battlespace and set conditions favorable to friendly force goals in case escalation into violence occurred (JP 3-13, 1998: II-9).

Table 2-2 Key Military Capabilities

Term	Key IO Concepts
Operations Security (OPSEC)	Seeks to deny the enemy access to critical information about friendly force capability and intentions in order to slow enemy decision processes. Requires knowledge of enemy's intelligence systems and the time required for information to reach decision makers.
Psychological Operations (PSYOP)	Actions taken to "convey selected information and indicators to foreign audiences" in order to influence emotions, motives, reasoning and behavior.
Military Deception	Affects enemy decision makers' intelligence collection, analysis, and dissemination systems in order to cause specific behavior based upon inaccurate impressions of the situation. This requires precise knowledge of the enemy and his decision making process.
Electronic Warfare (EW)	Any military action involving directed energy or electromagnetic weapons to control the electromagnetic spectrum. EW consists of Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES).
Physical Attack / Destruction	Operations involving traditional "hard kill" weapons against targets as part of an overall IO effort (i.e. communications lines connecting information systems).
Computer Network Attack (CNA)	Actions taken to deny, disrupt, degrade, or destroy information or information systems and / or the computer systems in which the information resides.
	Source: JP 3-13, II-3 – II-6, B-C-1, GL-5

All levels of IO require intelligence support. Intelligence collection sources must be broad-based, including both covert, national-level operations and open sources such as the media, commercial contacts and publications, academia, the Internet, and resident foreign nationals (JP 3-13, 1998: II-12). Intelligence processes must be in place to collect, store, analyze, and retrieve information needed to support IO in a timely manner (JP 3-13, 1998: II-11). One key area of intelligence support is Intelligence Preparation of the Battlespace (IPB), a continuous process used to develop detailed knowledge of adversary information and information systems. This includes

- Technical knowledge of a wide number of information systems;
- Knowledge of adversary political, economic, social, and cultural influences;
- Template development to portray the battlespace, and refine targets and methods for offensive IO COAs;
- An understanding of the adversary's decision making processes (content and timelines);
- An in-depth understanding, including motivations and leadership styles, of key adversary leaders, decision makers, and advisors; and
- Knowledge of geography, atmosphere, and littoral influences as they apply to the AOR (JP 3-13, 1998: II-12 – II-13).

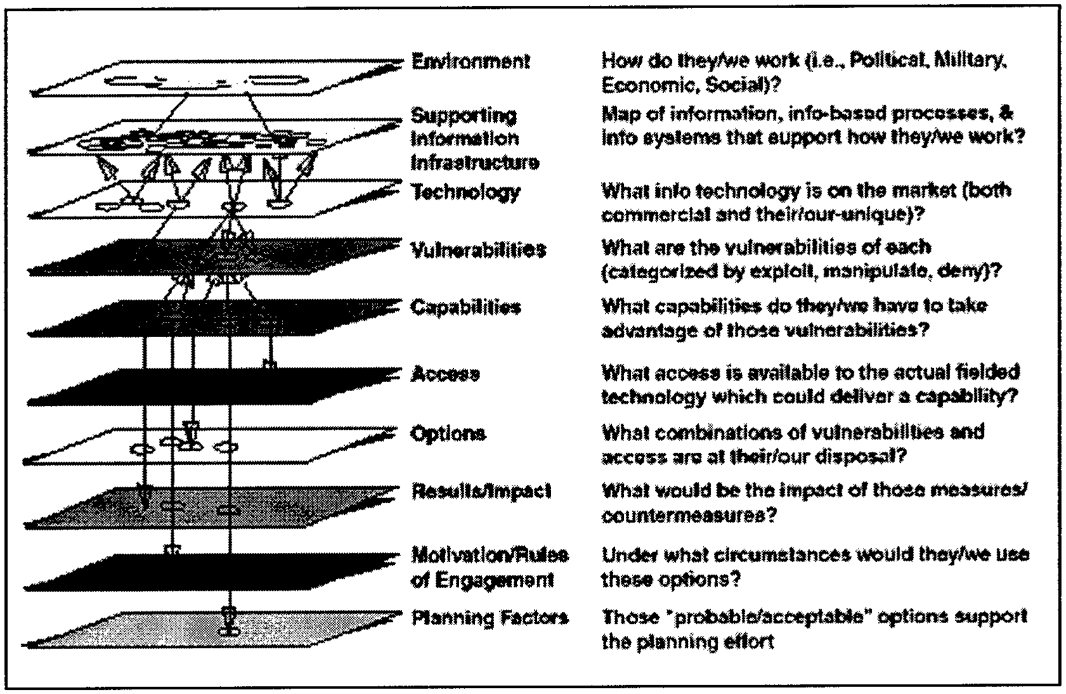
Section 4 of Chapter III in JP 3-13 deals with IO attack detection. It provides concepts and ideas that should be included in the hacker mentality model being developed. For example, not only must potential adversaries and their capabilities be identified, but their potential ability to affect friendly forces' information and information systems must be determined (JP 3-13, 1998: III-10). Intelligence activities provide warnings and assessments of potential adversary actions and cue intelligence collection to specific activity indicators (JP 3-13, 1998: III-10). This could include technological developments, threats to friendly force military, political, or economic interests, forewarning of actions or intentions of adversaries, or notice of imminent hostilities (JP 3-13, 1998: III-11).

Effective and properly focused response to IO attack requires timely identification of potential adversaries and their intents, with analytical results linked to decision makers. Traditional indications and warnings (I&W) must be expanded to better reflect unique characteristics of IO (JP 3-13, 1998: III-11). Some of the traditional I&W include adversary, or potential adversary,

- Capabilities;
- Intentions, preparations, deployments and related activities, and potential IO attack methods;
- Motivations, goals, and objectives;
- Changes in force dispositions, military and nonmilitary activities that could support IO; and
- Required mobilization preparations required to initiate IO and mobilization status (JP 3-13, 1998: III-11 – III-12).

The last sections of JP 3-13 deal with organization of Information Operations elements and IO planning. Doctrine stresses that IO organizational structure should be flexible, meeting the needs of a wide range of planning and operational situations (JP 3-13, 1998: IV-1). IO planning consists of both deliberate and crisis action planning. Deliberate plans are laid during peacetime in anticipation of subsequent need for IO during war and MOOTW (JP 3-13, 1998: V-1). They provide a general guide to IO planning for potential future crises (JP 3-13, 1998: V-6). Crisis action planning deals with quickly arising, unplanned for contingencies, and hence have a compressed time schedule (JP 3-13, 1998: V-6).

IO planning requires clear national strategic guidance to combatant commanders (JP 3-13, 1998: V-1). Commanders must then provide IO planners guidance on constraints, restrictions, and assumptions. This establishes boundaries for IO plans, provides policy limits on target identification, and reduces uncertainty in the planning process (JP 3-13, 1998: V-1-V-2). Planners must analyze the risks of compromise, adversary reprisal, collateral damage, and hostility escalation associated with IO (JP 3-13, 1998: V-1). An orderly process and schedule for decision making relating to IO is also required. Aspects of IO can require long-term development of intelligence and IPB, often beginning in peacetime (JP 3-13, 1998: V-2). In some cases, IPB for IO may require more lead time and/or have expanded collection requirements than traditional operations (JP 3-13, 1998: V-3). Figure 2-3 illustrates key steps in IO planning.



Environment	How do they/we work (i.e., Political, Military, Economic, Social)?
Supporting Information Infrastructure	Map of information, info-based processes, & info systems that support how they/we work?
Technology	What info technology is on the market (both commercial and their/our-unique)?
Vulnerabilities	What are the vulnerabilities of each (categorized by exploit, manipulate, deny)?
Capabilities	What capabilities do they/we have to take advantage of those vulnerabilities?
Access	What access is available to the actual fielded technology which could deliver a capability?
Options	What combinations of vulnerabilities and access are at their/our disposal?
Results/Impact	What would be the impact of those measures/ countermeasures?
Motivation/Rules of Engagement	Under what circumstances would they/we use these options?
Planning Factors	Those "probable/acceptable" options support the planning effort

Figure 2-3 Templating IO Planning and Assessments (JP 3-13, 1998: V-4)

IO planners must identify adversary strengths and vulnerabilities, identify opportunities and means to exploit vulnerabilities, and devise tasks and subtasks to accomplish objectives (JP 3-13, 1998: V-3). Identification of adversary strategic and operational centers of gravity is fundamental to IO planning. Finally, Two levels of approval authority are required for IO tasks. Release authority provides approval for use of IO and generally specifies means and capabilities provided to the execution authority. Execution authority is the actual authority to conduct IO at a given time and/or place (JP 3-13, 1998: V-3).

2.1.2. AFDD 1 – Air Force Basic Doctrine

AFDD 1 is the primary statement of US Air Force basic doctrine. It is meant to provide a common basis upon which airmen base their decisions (AFDD 1, 1997: 1). Doctrine consists of fundamental principles that guide the military actions in support of national objectives (AFDD 1, 1997: 1).

Three levels of air and space doctrine exist. Basic doctrine, such as that in AFDD 1, states the "most fundamental and enduring beliefs that describe and guide the proper use of air and space forces" (AFDD 1, 1997: 2). As a result, it provides broad guidance on how the Air Force is organized and employed (AFDD 1, 1997: 2). Operational doctrine provides more detailed guidance on the organization of the AF and applies basic doctrine to military actions (AFDD 1, 1997: 2). It shapes basic doctrine to a distinct set of objectives, force capabilities, functional areas, and operational environments (AFDD 1, 1997: 2). Finally, basic and operational doctrines provide a focus for the development of missions and tasks executed by tactical doctrine. Tactical doctrine "describes how weapon systems are employed to accomplish tactical objectives" (AFDD 1, 1997: 3). It considers specific tactical objectives and conditions.

Political, economic, and social situations may dictate that strategic and operational plans differ from accepted doctrine for particular contingencies. This illustrates the difference between doctrine and strategy. "Military doctrine describes how a job should be done … strategy defines how it will be done." (AFDD 1, 1997: 4)

AFDD 1 lists three enduring elements that describe the nature of war (AFDD 1, 1997: 6). First, "war is an instrument of national policy". As clearly seen in Vietnam, political objectives shape the scope and intensity of war. Second, "war is a complex and chaotic human endeavor". The nature of war is shaped by human characteristics such as frailty and irrationality, the "fog of war". Third, "war is a clash of opposing wills". This aspect of the nature of war captures the unpredictability of a human opponent. The will of both leadership and the nation as a whole will be tested by war. The will to prosecute or resist can be a key element of success (AFDD 1, 1997: 6).

War can be described in many ways. It does not require a formal declaration of war for the military to be engaged in combat (AFDD 1, 1997: 7). In many cases, operations are not conducted as a declared war, or even a preplanned contingency (AFDD 1, 1997: 7).

> War is a multidimensional activity that can be categorized in various ways: by intensity (low to high); by duration (short or protracted); by the means employed (conventional, unconventional, nuclear); or by the objectives/resources at stake (general or limited war) (AFDD 1, 1997: 7).

Regardless of the specific form of war being waged, nine "principles of war" have been seen to hold true. These are unity of command, objective, offensive, mass, maneuver, economy of force, security, surprise, and simplicity. The principles of war are generally accepted "truths" that remain self-evident over time. Table 2-3 Principles of War summarizes the key elements of these principles of war.

Table 2-3 Principles of War

Principle	Concepts
Unity of Command	All efforts are focused toward a common objective, and are directed by a single commander.
Objective	Military operations should support clearly defined and attainable objectives that contribute to strategic, operational, or tactical goals.
Offensive	One seeks to dictate the time, place, purpose, scope, intensity, and pace of operations.
Mass	Combat power should be focused at a decisive time and place to achieve optimum results.
Maneuver	The enemy is placed at a disadvantage by flexible application of combat power.
Economy of Force	Forces should be allocated in the best mix to support primary objectives.
Security	Forces should be protected from enemy actions that might provide the enemy an unexpected advantage.
Surprise	Attacks should come at a time, place, and/or manner for which the enemy is not prepared.
Simplicity	Military operations should avoid unnecessarily complex plans, organizations, and guidance.
	Source: AFDD 1, 12-21

Many of these principles have special bearing on the conduct of IO. For example, as with air and space power, IO does not require the achievement of tactical objectives before operational and strategic level objectives are pursued (AFDD 1, 1997: 13). The principle of objective seeks to avoid dividing IO forces to support fragmented objectives. IO and IW can greatly impact battlespace operations by seizing and maintaining the initiative. The goal is to force the enemy to react, denying them the offensive, and thereby shaping the future of the battlespace (AFDD 1, 1997: 15). This is why IO, as mentioned in JP 3-13, is a key element at the beginning of a crisis or MOOTW.

Mass in IO does not require concentration of forces in one location. Rather, forces can wait to combine at the target site (AFDD 1, 1997: 16). This is what makes Distributed Denial of Services (DDOS) attacks so "deadly". DDOS is a form of "parallel attack", which places maximum stress on enemy defenses by presenting multiple crises in quick succession so that there is no way to respond (AFDD 1, 1997: 24). The effect of mass for air, space, and IO forces is through efficiency of attack. "IW can, with precision, stealth, and the speed of light, affect a variety of functions and capabilities". (AFDD 1, 1997: 16) The principle of maneuver is tied to that of mass by the flexibility, versatility, and speed of air, space, and IO forces, allowing simultaneous application of both (AFDD 1, 1997: 17). Maneuver forces the enemy to react, since they do not know from what direction an attack might come. With these strengths of IW comes a warning in the form of economy of force. The contribution of IO and IW can be greatly diminished by misuse and misdirection of forces (AFDD 1, 1997: 18). Objectives and priorities should be clearly defined.

The principle of security presents interesting challenges to the DoD. Traditionally, security was enhanced by remaining out of reach of the enemy whenever possible. As discussed in Strategic Information Warfare: A New Face of War, IO can allow enemies the opportunity to strike at forces no matter where they are located. IO has overcome even the traditional sanctuary of the continental US. Additionally, the data and communications lines, rapid global mobility, and agile combat support that friendly forces rely on for information and analysis, movement of forces and supplies, and logistic support in theater can be attacked at any point in their transmission from supplier to customer. However, successful security measures conceal friendly force capabilities and intentions, allowing freedom of movement to gather information on the enemy.

The other side of the coin from security is the element of surprise. IO and IW contribute to this principle since they are not inhibited by concepts such as distance or terrain (AFDD 1, 1997: 20). Force buildups in the realm of cyberspace are not as readily noticed as traditional forces on the battlefield. As a result, it is harder to notice when an attack has actually occurred, and from whence it came. Finally, plans, organizations, and operations should be simple. This allows lower level commanders an element of freedom in adapting to the battlespace as the situation dictates (AFDD 1, 1997: 21). IO and IW, to be successful, must have freedom to react at the speed of the crisis or MOOTW, without resorting to complex organizational frameworks and guidance.

A final concept for this effort from AFDD 1 is the core competency of Information Superiority. This concept is similar to the concepts of air and space superiority – one seeks to gain control over the information realm in order to fully exploit friendly force information functions while denying those capabilities to the enemy (AFDD 1, 1997: 31). "Whoever has the best ability to gather, understand, control, and use information has a substantial advantage." (AFDD 1, 1997: 32) Information Superiority shapes the adversary's perception of the situation and available courses of action, and degrades and/or influences their decision making processes (AFDD 1, 1997: 32). AFDD 1 cautions that in seeking Information Superiority we must not expect our adversaries to react with the same values, preferences, frames of reference, and strategies that we have developed (AFDD 1, 1997: 40).

2.1.3. AFDD 2-1.5 Nuclear Operations

While it may seem strange to refer to doctrine on nuclear weapons when discussing IW, AFDD 2-1.5 addresses how the Air Force views the concept of deterrence. Similar views could be expressed for a concept of IW deterrence; an idea that was suggested by Chinese author Shen Weiguang in a February 2, 1999 article in *Jiefangjun Bao* (Farris, 2000: 38 – 39). Farris quotes Mr. Weigung as having written, "Only when we possess the capability to win, and make preparations to win, can we possibly realize the aim of checking the warfare."

The focus of AFDD 2-1.5 is to "maintain effective forces with sufficient capability to hold at risk a broad range of targets, while placing great emphasis on safety and security" (AFDD 2-1.5, 1998: v). The goal is a credible posture for deterrence based on posturing, maintaining, and exercising capable forces, as well as having the intent to employ those forces if efforts in deterrence fail (AFDD 2-1.5, 1998: vi).

Deterrence is defined as

> … a state of mind created in an adversary's (or potential adversary's) leadership. Their leadership must believe the cost of aggression against the United States, its interests, or its allies will be so high as to outweigh any possible gain. … If an enemy believes these tools will not be used, then their deterrent value is zero (AFDD 2-1.5, 1998: 2).

As with nuclear weapons, the impact of an IW activity can produce political and psychological effects far beyond the actual physical effects. Often it may be hard to determine what these effects might be for nuclear weapons (AFDD 2-1.5, 1998: 11). The same could be said for the emerging concept of IW. One example is the effect that these weapons might have on relations with other nations once they are known to exist or are used (AFDD 2-1.5, 1998: 11). This could justify the US treating IW on the same plane as nuclear, biological, and chemical (NBC) weapons, but does not mean that potential adversary's will treat IW in the same fashion. Similarly, the potential for severe collateral effects and unintended consequences has lead to decisions of whether to use, or threaten to use, nuclear weapons being strictly political (rather than military) (AFDD 2-1.5, 1998: 1). The US may also decide that, at some levels, IW weapons could also require the same caution in their use.

Since the key to deterrence is to target those things that an adversary most values, target selection is based both upon friendly force objectives and enemy objectives (AFDD 2-1.5, 1998: 8). If deterrence fails, targets that could bring a quick end to hostilities are preferred. Those developing target sets must consider both their own view of the targets, as well as the perspective of the enemy state (AFDD 2-1.5, 1998: 8). Two targeting strategies are countervalue and counterforce. Countervalue targeting "involves holding enemy cities, industry, and other economic resources at risk" (AFDD 2-1.5, 1998: 8). The goal is large casualties in the short-term, as well as long-term degradation of the adversary's society (AFDD 2-1.5, 1998: 8). On the other hand, counterforce targets are more limited. They constitute targeting of an adversary's immediate ability to wage war, seeking an "immediate operational effect" (AFDD 2-1.5, 1998: 8). This could consist of actual targeting of enemy troops, weapons stockpiles, planes on the ground, or similar targets. IW attacks can operate at either the countervalue or counterforce level.

Two final areas of common doctrinal concern between nuclear and IW operations are the Law of Armed Conflict and war termination. Both will be briefly discussed as IW doctrine must address them, but they are not a focus of this study. The Law of Armed

Conflict is based upon a broad group of treaties, customs, and national practices regarding how war is waged. "This body of international law protects combatants and noncombatants, safeguards human rights, and facilitates the achievement of peace by limiting the amount of force and the manner in which it can be applied." (AFDD 2-1.5, 1998: 8). While the idea of counterbalancing military need, proportionality, distinction, and avoidance of unnecessary suffering has been readily applied to nuclear weapons, the concept must be explored for IW. A computer virus released by a country in time of war may have far-reaching and devastating effects upon the world at large.

For the concept of war termination, the goal of nuclear operations is "to achieve US political objectives and resolve conflict on terms favorable to the United States" (AFDD 2-1.5, 1998: 12). IW, emerging as a new form of war, will have the same goal. Combat assessment is a tool to determine when to continue or when to terminate a war or Military Operation Other than War (MOOTW). The three components of combat assessment are battle damage assessment, munitions effects assessments, and reattack recommendations. As with nuclear weapons, "intelligence analysts must understand, and collection assets must be designed to measure, the unique effects" of IW weapons (AFDD 2-1.5, 1998: 12). The Air Force could use combat assessment tools developed for friendly force offensive IW actions to gauge the potential effects of enemy IW actions and to develop defensive measures before these attacks are launched.

2.1.4. AFDD 2–5 Information Operations

AFDD 2–5 specifically addresses the Air Force perspectives on information warfare and information superiority. It provided the basic definitions of IO and IW presented in Chapter 1, and stresses the growing importance of IO in modern warfare.

Information superiority, domination of the information spectrum, is as critical to military success as the control of land, air, or space (AFDD 2-5, 1998: 1). Today, the Defense Information Infrastructure (DII) is partially reliant upon the National Information Infrastructure (NII), which is in turn connected to the Global Information Infrastructure (GII) (AFDD 2-5, 1998: 4). These interdependencies present opportunities for adversaries to infiltrate and attack any of the interconnected information systems rather than face the US's strength on the traditional battlefield (AFDD 2-5, 1998: 6).

Four threat areas for IW attacks by terrorists, criminals, and hackers are compromise, deception / corruption, denial / loss, and physical destruction (AFDD 2-5, 1998: 6 - 7). Based upon the work in RAND reports summarized in Section 2.1.5 and AFDD 2-5, Table 2-4 Information Warfare Threats presents examples of each of the four threat areas. Examples representing potential hacker attacks, or vulnerabilities that a hacker might exploit, are marked by an asterisk (*).

Table 2-4 Information Warfare Threats

Compromise	**Deception / Corruption**	**Denial / Loss**	**Destruction**
Malicious Code* System Intrusion* Psychological Operations* Intelligence Collection* Technology Transfer* Software Bugs*	Malicious Code* System Intrusion* Military Deception* Spoofing* Imitation*	Malicious Code* System Intrusion* Lasers Physical Attack Nuclear & Non-nuclear EMP Virus Insertion* System Overload* Radio Frequency Jamming	Malicious Code* Bombs Directed Energy Weapons Lasers Physical Attack Nuclear & Non-nuclear EMP Chemical / Biological Warfare
Source: AFDD 2-5	*areas exploitable	by hackers	

Defensive counterinformation (DCI) focuses on the need to protect information, information systems, and information operations from enemies (AFDD 2-5, 1998: 10). It encompasses such concepts as Information Assurance, Operation Security (OPSEC), Counterintelligence, Counter PSYOP (psychological operations), Electronic Protection, and Counterdeception (AFDD 2-5, 1998: 3). Defensive counterinformation is the Air Force's top priority within the IW arena (AFDD 2-5, 1998: 15). Deception operations attempt to mislead an enemy so that he or she acts according to the deceptor's intent (AFDD 2-5, 1998: 13). Counterdeception, therefore, seeks to help decision makers identify an enemy's deception attempts. A key factor in successful deception is an understanding of the cultural, political, and doctrinal framework that the intended target operates within (AFDD 2-5, 1998: 13). OPSEC focuses on limiting the information available to adversaries that could be used to derive critical information about DoD systems (AFDD 2-5, 1998: 16). Counterintelligence efforts focus on identifying and assessing vulnerabilities that could be exploited by an adversary (AFDD 2-5, 1998: 18). Social engineering attempts by hackers would represent a vulnerability that counterintelligence efforts would attempt to mitigate, possibly through personnel training. Finally, misinformation spread over the Internet would represent an attempt at psychological operations that Air Force Counterpsychological efforts would attempt to identify and mitigate.

When perpetrated by a military organization, a hack can be considered an information attack. "Information attack refers to those activities taken to manipulate or destroy an adversary's information or information system without necessarily changing visibly the physical entity within which it resides." (AFDD 2-5, 1998: 6 - 7) These attacks can affect decision making by denying access to information, degrading accuracy of decisions, or denying access to technology. It also reduces the exposure of conventional forces to harm (AFDD 2-5, 1998: 15). Such attacks could focus on strategic effects, operational effects, tactical effects, or a combination thereof (AFDD 2-5, 1998: 28 - 30).

As a prelude to exploring an adversary's IO goals during a conflict, it is useful to explore the strategic, operational, and tactical effects AFDD 2-5 identifies for Air Force operations during conflicts. Table 2-5 Air Force Information Operation Goals summarizes these goals.

Table 2-5 Air Force Information Operation Goals

Strategic Effects (national objectives)	**Operational Effects** (theater level)	**Tactical Effects**
- Influence ally and adversary behavior toward US national objectives - Terminate leadership resistance, reduce adversary's confidence, degrade communication capability - Deter aggression, support counterterrorism and counterproliferation	- Negate adversary's ability to strike - Reduce adversary's operational tempo - Negate adversary's command, control, communication, computer, and intelligence capabilities - Influence world support in favor of US objectives - Disrupt adversary's plans and focus - Disrupt adversary's decision process	- Prevent adversary's effects on friendly IO - Reduce size or capability of adversary forces - Deny adversary knowledge of friendly forces
Extracted from AFDD 2-5		

2.1.5. RAND Studies

The RAND Corporation has performed several research efforts for the Department of Defense (DoD) that deal specifically with the effects of the information revolution on the nature of war.

Strategic Information Warfare: A New Face of War

This study develops a framework to characterize strategic information warfare, and explores how information warfare can affect national security. The authors define strategic information warfare as an emerging type of conflict "wherein nations utilize cyberspace to affect strategic military operations and inflict damage on national information infrastructures" (Molander, Riddile, and Wilson, 1996: 1). In studying the concept of strategic information warfare and its effects upon future wars, RAND was tasked to focus on the defensive, rather than offensive, nature of the concept (Molander, *et. al*, 1996: 3).

The rapid spread of computer technology has changed the face of war. The number of potential enemies with the access to tools for waging strategic information warfare is large (Molander, *et. al*, 1996: 11). The theaters in which this new war might be waged are not just those of the traditional theater of operations – strategic information warfare can target any point in the chain of regions from the continental US, to deployment and redeployment zones, to anywhere surrounding the traditional theater of operations (Molander, *et. al*, 1996: 12). "Strategic IW reduces the significance of distance with respect to the deployment and use of weapons" (Molander, *et. al*, 1996: 42). According to the authors, US strategy in 1996 did not address the possibility that an adversary make attack all of these theaters (Molander, *et. al*, 1996: 37). The range of targets is also expanded. In addition to military, political, and economic targets, information warfare can target the social framework of a country itself. It is likely that enemies may avoid facing the US's technological superiority and strength of numbers in the field by attacking more vulnerable targets through asymmetric IW (Molander, *et. al*, 1996: 37). The US will no longer remain a sanctuary from war (Molander, *et. al*, 1996: 12).

Seven key features of strategic information warfare help define the difference between this new form of war and more traditional forms of conflict (Molander, *et. al*, 1996: 15 - 16).

Low Entry Cost

The low entry costs for IW facilitates the development of viable IW programs by a wide range of players, be they nation states, terrorists, or criminals. Additionally, new IW weapons can be developed with limited equipment, anywhere in the world, by technically knowledgeable adversaries (Molander, *et. al*, 1996: 15). The growing connectedness of computer systems in all aspects of governmental and commercial infrastructures provides multiple targets and attack paths. Finally, the ease with which potential adversaries can acquire the tools and talent necessary to build IW capabilities makes it difficult to identify and monitor possible sources of future attacks (Molander, *et. al*, 1996: 18).

Blurred Traditional Boundaries

The growth of the Internet has changed how people view the world, blurring the traditional boundaries between nations. This also blurs the distinction between what is a foreign or domestic source of IW threat (Molander, *et. al*, 1996: 19). The once fine distinction between criminal acts and anti-state activity may no longer exist as it becomes more difficult to identify "who gave the order" (Molander, *et. al*, 1996: 20). A final consequence is that during an attack it may be difficult to tell what is under attack, by whom, and, therefore, who has the responsibility to respond (Molander, *et. al*, 1996: 20).

Perception Management

Perception management also becomes more difficult in the realm of IW. The Internet provides a wonderful opportunity to rapidly spread information and disinformation worldwide. Militia groups have already capitalized on the Internet to build, support, and disseminate their views (Molander, *et. al*, 1996: 22). Political support in future conflicts will have to be won on the Internet as well as over traditional news media. The ability to publish disinformation on the Internet has lead to situations where the US leadership and the American public at large no longer know what is real (Molander, *et. al*, 1996: 23).

Strategic Intelligence

The previous areas of concern feed into the problem of obtaining good strategic intelligence. The traditional approach of focusing on specific nation states with distinct boundaries is no longer sufficient, as the low cost of IW raises the number of potential adversaries while their locations become blurred (Molander, *et. al*, 1996: 24). The list of potential adversaries has become dynamic, making it difficult to know their identity, capabilities, and intent (Molander, *et. al*, 1996: 25). The separation of domestic law enforcement and the intelligence community is seen as a factor hindering strategic intelligence collection in many cases (Molander, *et. al*, 1996: 26).

Tactical Warning and Attack Assessment

Tactical warning and attack assessment also becomes more difficult in IW. The speed of attacks and the ability to hide in cyberspace increases the difficulty of identifying and characterizing an attack in a timely manner (Molander, *et. al*, 1996: 26 - 27). In some cases, what appears to be a minor incident could be part of an ongoing intelligence effort in support of future operations. Additionally, the ability to determine whether an attack is an official act of war or not adds to leadership's problems in crafting an appropriate response (Molander, *et. al*, 1996: 27).

Building and Sustaining Coalitions

Building and sustaining coalitions also becomes more difficult in the Information Age. Conducting operations with other countries on foreign soil was complex enough before the use of IW adds to the fog of war (Molander, *et. al*, 1996: 28). In addition, allies may seek reassurance that the US plans are not subject to disruption from IW efforts, and the US may be concerned about allies' weaknesses as well (Molander, *et. al*, 1996: 29). Management and protection of coalition information systems becomes a key concern.

Vulnerability of the US Homeland

Finally, there is the inescapable fact that the US is no longer a sanctuary (Molander, *et. al*, 1996: 30). The growing dependence on interconnected computer infrastructures provides an adversary many vital targets, both commercial and governmental. Deterrence is more problematic since attacks at the speed of light can come from anywhere (Molander, *et. al*, 1996: 37).

Countering the New Terrorism

This RAND study focuses on how changes in the nature of warfare, from the advent of the information revolution to widespread availability of biological and chemical warfare agents, have also affected terrorism (Lesser, Hoffman, Arquilla, Ronfeldt, and Zanini, 1999: xv). Terrorism is defined as "a crime in the classic sense … albeit for political motives" (Lesser, *et. al*, 1999: v). Terrorism is also partially defined by the separation of the victims of the act from the intended audience (Lesser, *et. al*, 1999: v). Over time, terrorist acts have become more violent, in part due to the spreading ethnic and religious nature of the groups carrying them out (Lesser, *et. al*, 1999: vii). During this same period, terrorists organizations have reorganized themselves into more networked structures that make wider use of amateurs and members of other groups (Lesser, *et. al*, 1999: 1).

> "In the past, terrorism was practiced by a collection of individuals belonging to an identifiable organization that had a clear command and control apparatus and a defined set of political, social, or economic objectives. …their ideology and intentions were at least comprehensible – albeit politically radical and personally fanatical."
>
> (Lesser, *et. al*, 1999: 8).

Traditionally, terrorist groups were selective in their targets, focusing on those symbolic of the source of their anger, and controlled in their use of violence (Lesser, *et. al*, 1999: 8). Connections to foreign governments were vaguely recognizable, if not well substantiated (Lesser, *et. al*, 1999: 8). In more recent years, new terrorist groups have emerged that are much less well defined. Their memberships are less restricted, as are their aims, while at the same time their membership numbers have grown beyond the size of older terrorist organizations (Lesser, *et. al*, 1999: 9 - 10). Sponsorship by nation states is still a force multiplier for terrorist groups – "enhancing planning, intelligence, logistical capabilities, training, finances, and sophistication" (Lesser, *et. al*, 1999: 15). In effect, terrorists become "surrogate warriors", adding an asymmetric force to any actions against the US (Lesser, *et. al*, 1999: 15). Many of the newer terrorist organizations are now classified as religious in nature, and the religious ideology is often tied to an increase in violent acts made justifiable by religious imperatives (Lesser, *et. al*, 1999: 17 - 20).

The amorphous, transitory nature of the new terrorist organizations, compounded by the wealth of information available over the Internet or through books, mail-order, or CD-ROM, increases the difficulty in identifying, tracking, and understanding the various groups (Lesser, *et. al*, 1999: 20 - 22). Often no central command authority exists, and in some cases a group forms for a specific, perhaps even one-time, purpose (Lesser, *et. al*, 1999: 21 - 22). There is still the chance that these loosely coupled groups are indirectly influenced or controlled by nation states or nongovernmental entities (Lesser, *et. al*, 1999: 22). Combined with the low cost of IW tools and the inherently expendable nature of the terrorist group, this could allow these nations to act against the US without fear of direct reprisals or diplomatic and economic sanctions (Lesser, *et. al*, 1999: 23).

The advent of the information age may have changed the way that terrorists view their world. The past focus on individual acts as a way to coerce results may now be moving to a view of terrorism as a protracted form of unconventional warfare (Lesser, *et. al*, 1999: 39). The idea of unconventional warfare appeals to those viewed traditionally as weaker than their adversaries, those seeking to gain attention to themselves and their cause, and as a way of moving to a future world by destroying the present (Lesser, *et. al*, 1999: 39 - 40). To support these goals, terrorists are changing to a less hierarchical, more networked structure, often connected over the Internet (Lesser, *et. al*, 1999: 41). Systemic disruption, provided by IW tools such as Denial of Service (DoS), is becoming more of a focus than target destruction (Lesser, *et. al*, 1999: 41). Finally, terrorists are making use of information technology and the tools it provides to support themselves both offensively and defensively (Lesser, *et. al*, 1999: 41).

The authors use the term "netwar" to describe the direction in which they see terrorism moving, with examples provided in the actions of Middle East terrorist groups (Lesser, *et. al*, 1999: 41). Netwar is differentiated from "Cyberwar" by the level of perceived intensity and realm of action– netwar is low-intensity and societal in nature, while cyberwar is high-intensity and military in nature (Lesser, *et. al*, 1999: 46). Additionally, cyberwar is seen as the application of new technology to existing concepts of warfare, while netwar is seen as the emergence of an entirely new form of warfare (Berger, 1998: 112). Two tiers of terrorists are emerging – one of professionals and the other of amateurs (Lesser, *et. al*, 1999: 43). At times, the professional groups may hide behind the actions of amateurs. Both groups already see information infrastructures as key targets (Lesser, *et. al*, 1999: 44). Information technology allows the potentially dispersed groups to launch coordinated attacks against these targets from considerable distances (Lesser, *et. al*, 1999: 45).

The networked structure of netwar actors takes advantage of the flexibility and adaptability of networks. Communication is facilitated by the organizational structure, decentralization is common, and initiative and autonomy are often encouraged (Lesser, *et. al*, 1999: 51). Nodes within the structure may be large or small, tightly or loosely couples, and are often non-state actors (Lesser, *et. al*, 1999: 48 - 50). To be successful, a core set of shared principles, ideas, or goals are required, along with a method of rapidly spreading information to members as well as, potentially, the world at large (Lesser, *et. al*, 1999: 51). The Internet, e-mail, and cell phones provide the required tools. New, younger members of terrorist organizations have grown up with these technologies, and can lend their expertise to the group (Lesser, *et. al*, 1999: 67 - 68).

More in the realm of cyberwar, adversaries may use IW as an asymmetric strategy against the US and its allies. Terrorism could be seen as a way to gain time to consolidate land grabs, to directly attack the US or one of its allies, or to wage war in the battle for the American public (Lesser, *et. al*, 1999: 94). The authors feel that IW based terrorist attacks may become the norm rather than the exception in the future (Lesser, *et. al*, 1999: 95). These attacks are more of a concern for the developed nations of the world, who are increasingly relying on information systems to control their infrastructure. The driving factors for these future IW incidents are seen as to fit the following categories:

- Ethnic Separatism and Frustrated Nationalism;
- Religious Extremism and "Postmodern" (apocalyptic) Terrorism;
- Low-Intensity Product of Regional Rivalries;
- New Ideological Clashes (i.e. over class or economic distinctions);
- Crime and Drugs;
- Losers of Confrontation with the US and its allies; and,
- Anarchy and Rage (Lesser, *et. al*, 1999: 99 - 109).

2.1.6. Organizational Innovation and Redesign in the Information Age: The Drug War, Netwar, and Other Low-End Conflict

Berger's thesis explores the effects of organizational structure on success in the Information Age. The relationship between an organization's structure, and its ability to act and react, will have a bearing on the hacker profiles being developed in Chapter 3 of this study. Berger postulates that organizations that move to a networked structure will be more flexible, adaptable, and innovative, and will therefore make quicker decisions and be more successful than organizations that still follow a hierarchical approach (Berger, 1998: x). On the military front, the traditional, hierarchically organized threat is evolving into less formally organized, threats (Berger, 1998: 3). The two hypotheses of interest are 1) "The future security environment will not be one of peace or war, but different "degrees" of conflict" and 2) "The new security environment will consist of traditional military threats, but will also include numerous threats that aren't currently dealt with by current defense structures" (Berger, 1998: 3).

The case study Berger used to explore these hypotheses is the international drug war. It is seen as an example of the conflict between nations and transnational organizations not limited by international boundaries or laws (Berger, 1998: 7). In this case, Berger states that the threat is not to national stability, but to the confidence and faith of the American public (Berger, 1998: 7).

Organizational theory provides the basis for exploring Berger's hypotheses. One focus is on the paradigms with which an organization approaches the world. These paradigms are influenced by biases, past experiences, cultural issues, and other factors that impact on decision making (Berger, 1998: 7). These concepts will also be important in exploring the framework of malicious hackers. Organizational theory provides a "rational-systems model" that finds the best structure for a given organization based upon goals, roles, and technology (Berger, 1998: 21). Interrelated system aspects are strategy, structure, processes, people, and rewards. A change in one system aspect requires evaluation, and possibly changes, in the other aspects (Berger, 1998: 21). Environmental pressures may also require system changes (Berger, 1998: 22).

Berger found that transnational criminal organizations and terrorist groups are incorporating vertical information processing and lateral relations, often supported by information technology, to improve information flow at all levels (Berger, 1998: 27). The idea of vertical information processing seeks to provide all levels of command the same information. This can be seen in the military's focus on developing "system of systems" to integrate a variety of information sources for use by all levels of command (Berger, 1998: 26). Development of lateral relations means decentralization, where decision making authority is passed as far down the chain of command as possible (Berger, 1998: 25). Decentralization can also encourage information sharing across lines of authority (Berger, 1998: 25).

While criminal and terrorist groups are evolving into more networked organizational structures, the military still depends on a traditional hierarchy which can make it slower to respond to change. Hierarchies are most effective in situations where little environmental uncertainty exists (Berger, 1998: 29). On the other hand, organizations that use project team or organic network structures require little formal coordination, encourage innovation, allow greater informal information flow, and can more readily deal with large amounts of environmental uncertainty (Berger, 1998: 33 - 35).

Examples of organic network structures used by organizations are all-channel (everyone can talk to each other) and chain or star structures that allow less interconnectivity. Organizations might combine an all-channel core command structure and star or chain structures for lower level functions (Berger, 1998: 36). A change from a hierarchical structure to a more networked structure requires cultural as well as structural changes (Berger, 1998: 37).

Berger uses international drug cartels and the governmental agencies that pursue them as a case study in organizational structure. Over the past few decades, these cartels, which are loose confederations of different drug trafficking groups, have moved across the spectrum of organizational structures from independent hierarchies to interdependent networks (Berger, 1998: 60 - 61). "Their boundaries are fluid, the cast of characters change continually, and the links in the chain are bound together by an intricate system of contracts and subcontracts." (Berger, 1998: 72)

In part, the advent of information technology has aided this evolution; speeding and expanding the communication network through use of cell phones, fax machines, pagers, and e-mail (Berger, 1998: 72, 76). Even when the "head" of a cartel is arrested or killed, the loose network structure survives since pieces of the network, to include the locations of operations, can be removed or replaced as required (Berger, 1998: 75). This flexibility contributes to law enforcement's difficulties in closing the drug trade.

Cartels also use high technology to gather intelligence on counternarcotics operations. Berger asserts that cartels' intelligence efforts are very similar to national-level intelligence agencies, frequently recruiting insider support through threats and bribery (Berger, 1998: 78 - 79). As smaller cartels have grown to replace the larger ones of the past, one telling difference has emerged. Older cartel leaders sought recognition as societal figures; new cartels show interest only in financial gain (Berger, 1998: 86).

One of the main challenges for law enforcement is the international level of drug operations. It remains difficult to share intelligence across national boundaries (Berger, 1998: 96). This same difficulty arises in the pursuit of hackers. Limitations on the amount and types of information that can be shared across agencies at all levels, and the lack of appropriate infrastructures to support information exchange, hinder law enforcement (Berger, 1998: 96). Berger also asserts that the US national security structure stifles innovation by its bureaucratic nature, and that it is predictable (Berger, 1998: 98). The decentralized nature of the cartels, combined with their extensive communication structure, allows the cartels to spread information more quickly than law enforcement (Berger, 1998: 100).

The Cold War, with its relatively stable environment and predictable threats, contributed to the hierarchical nature of the US national security structure (Berger, 1998: 104). The current state of global affairs is no longer stable, with any number of state or non-state actors possessing the potential to become adversaries at any time. The Information Revolution contributed to this change by helping smaller or less efficient groups increase their ability to communicate and attack with greater security and ambiguity (Berger, 1998: 107). This change is also seen in the blurring of the bounds between foreign and domestic threats, challenges to national security and criminal activity (Berger, 1998: 110).

Berger also discusses the concept of Netwar. Non-state actors rely on networked organizations with little centralized command or hierarchy. While they do follow a central doctrine, they are operationally decentralized and reliant on rapid communication with all parts of the organization (Berger, 1998: 112 - 113). These organizations, which exist at levels from sub-national to transnational, depend upon consensus building for decision making, allowing local initiative and autonomy (Berger, 1998: 115). Organizational success is the result of a shared sense of purpose (Berger, 1998: 115). "Offensively, netwar organizations are adaptable, flexible, and versatile in their response to challenge." (Berger, 1998: 121) Decentralization encourages innovation, allowing a netwar organization to better exploit an adversary's weaknesses, learn from its own mistakes, and institutionalize change more rapidly (Berger, 1998: 121).

Terrorists, which have traditionally used decentralization to operate and maintain secrecy, are taking advantage of information technologies to increase communication while decreasing the risk of discovery (Berger, 1998: 116). Strategic alliances, based upon shared goals or ideologies, are common for both the drug cartels and netwar organizations. These alliances may even involve state actors, such as state support for terrorists groups (Berger, 1998: 119). These loose alliances may be based upon a specific goal or evolve into long-term organizational changes (Berger, 1998: 119).

While US national security organizations are responding to the threat of cyberwar and netwar, they are doing so with the traditional hierarchical structure (Berger, 1998: 133). The broad and ambiguous nature of world threats makes identification of potential adversaries and prediction of their future actions more difficult (Berger, 1998: 138). The intelligence community must not only determine the capability of future cyberwar and netwar adversaries, they must also attempt to determine intent and motivation. With limited historical information on the groups of interest, the job is becoming more difficult (Berger, 1998: 139). An additional problem is the regional / global nature of non-state threats on the Information Age. These groups can move freely across international borders that nation seeking to respond to a threat or an attack must respect (Berger, 1998: 142). Adversaries that know the legal constraints find innovative ways to use the laws to their advantage. For example, US national intelligence organizations are prevented from collecting against US citizens anywhere in the world. A drug cartel that requires all communications involve one American ensures that intelligence agencies are thwarted; unfortunately, in most cases law enforcement agencies do not have the equipment necessary to collect the intelligence (Berger, 1998: 148).

2.2. Legal Issues

There are several legal issues that affect how the military and law enforcement agencies deal with hackers. One of the first issues is the *Posse Comitatus* law, which prohibits use of the military for law enforcement within the US borders. Incidents and intrusions regarding DoD systems should be reported to military criminal investigators and counterintelligence agents so that appropriate action is taken. Internal DoD procedures balance the needs of incident investigation with protection of information integrity and individual privacy rights (JP 3-13, 1998: III-10). Records from past incidents are a vital element in identifying and defining vulnerabilities, which leads to security improvements (JP 3-13, 1998: III-14).

2.2.1. JP 3-13

JP 3-13 acknowledges the complex legal and political nature potentially involved in IO. Legal limitations may vary depending upon the current level of war, and with the offensive or defensive nature of a specific IO (JP 3-13, 1998: I-12). IO planners are advised to consider three broad areas of concern. First are the limitations of domestic and international criminal and civil laws regarding national security, personal privacy, and issues of information exchange and ownership. Second are concerns with international treaties and agreements, and customary international law that might affect IO. For example, restrictions may be placed on tracing a hacker through servers that belong to private corporations and that reside in a foreign nation. Third are issues of formal and informal relationships among US intelligence agencies, other US agencies and organizations, and nongovernmental organizations (JP 3-13, 1998: I-1).

Diplomatic actions and economic sanctions may prove useful in cases where attacks can be tied to nation states. Diplomatic actions, in addition to their deterrent value, provide low cost, scaleable, and easily adjusted options for attack response (JP 3-13, 1998: III-14-III-15). While economic sanctions can prove troublesome to enforce, they may weaken an adversary to the point that they become susceptible to other response options (JP 3-13, 1998: III-15). Finally, military force provides a wide range of lethal and nonlethal response options that may eliminate a threat directly or interrupt an adversary's means of conducting IO (JP 3-13, 1998: III-15).

2.2.2. DoD Office of the General Counsel

The Office of the General Counsel has begun to address the legal issues surrounding IO as they apply to the military. When it comes to issues of law, sovereign nations are of equal status. Therefore, it is only through agreement that they assume legal obligation to each other (DoD General Counsel, 1999: 1). The General Counsel makes the assertion that international law develops to handle the situations at hand (DoD General Counsel, 1999: 1). Efforts to develop strong restrictions on IO would follow incidents that cast IO as a severe, revolutionary threat to national security.

Hacking, termed computer network attack (CNA) when used by a nation state, is seen as significantly different from traditional weapons. As such, current international law does not provide existing legal principles that easily apply (DoD General Counsel, 1999: 5). The very nature of the attacks, which can come from anywhere and which may leave few traces of the intruder, raises questions as to attribution, intent and motive, and the application of international law dealing with territory invasion and attacks by traditional troops and weapons systems (DoD General Counsel, 1999: 5).

As mentioned in JP 3-13, the laws of war must also adapt to IO and IW. The distinction between noncombatants and lawful combatants is much less clear when those involved may never see each other (DoD General Counsel, 1999: 8). Military necessity as balanced against attacks on civilian entities is also a more contentious issue (DoD General Counsel, 1999: 8). Targeting of a nation's economy will most likely shorten a war, but the interlinked nature of the global economy poses a high chance of collateral, possibly worldwide, damage. For short duration conflicts, justification of such a target may be harder to support. The concept of proportionality in IO attacks poses similar problems (DoD General Counsel, 1999: 9). Collateral damage can be a large risk. For example, computer viruses could be an effective weapon, but their ability to spread without bounds could result in more harm to civilian systems than is justified by military advantage. Viruses could represent an indiscriminate weapon (depending on how they are written), as could attacks on computer systems that result in loss of control of dams, refineries, or power stations. Indiscriminate weapons are forbidden by the laws of war (DoD General Counsel, 1999: 9).

Even the issue of neutrality must be considered for communications relay systems existing in neutral countries (DoD General Counsel, 1999: 10). An extension to the exception for telegraph and telephone lines could apply. In this case, as long as the neutral nation provides the same access to both sides of the conflict, neutrality is maintained (DoD General Counsel, 1999: 10). The same exception, according to the General Counsel, would not apply to systems that create information.

While the concept of an act of war has fallen out of favor according to the General Council, IW attacks would most likely be seen as acts of aggression – a "crime against the peace for which there is a responsibility under international law" (DoD General Counsel, 1999: 12-13). The General Counsel states that a single incident of CNA may not be treated as an act of aggression, unless it results in widespread damage (DoD General Counsel, 1999: 15). They feel that how the incident is viewed would depend in part on the intent and consequences of the attack (DoD General Counsel, 1999: 18). If a CNA is determined to represent an act of aggression, the victim nation is entitled to respond. This raises questions as to the appropriate response, since the exact equipment and personnel involved may not be easy to identify (DoD General Counsel, 1999: 18).

2.2.3. News articles

The Council of Europe has begun work on a cyber crime treaty, with all forty-one nations participating in the effort. The treaty calls for "increased, rapid, and well-functioning international cooperation" on the issue (Meller, 2000). One of the concerns of the treaty is the use of computer networks and the information they hold to commit crimes, as well as the evidence relating to the crime that may be stored or transmitted on these networks (Meller, 2000). The issue of extradition will also be addressed in the treaty, easing the prosecution of any criminals who are citizens of those nations supporting the treaty (Meller 2000). Finally, the treaty is seen to be most useful in the lesser developed nations of the Council of Europe, as the more develop nations tend to have laws against cyber crime already in place (Meller, 2000). International actions such as this treaty could provide the basis for extending the laws of war, as well as domestic and international laws and policies, to IW.

In 1997, The US, Britain, Canada, France, Germany, Italy, Japan, and Russia pledged to coordinate efforts to combat cyber crime (Denning, 1999: 395). The agreement involves cooperation in the search and prosecution of cyber criminals from each other's countries. Additionally, it encourages the development of technology to support the efforts of law enforcement, to include obtaining and sharing witness testimony (Denning, 1999: 395).

2.2.4. Legal issues in <u>Hackers</u> by Taylor

Taylor asserts that two camps exist with respect to dealing with hackers – the hawks and the doves. Hawks oppose dealing with hackers other than through legal prosecution efforts. They do not feel that hackers can or should contribute to improving computer security. Doves, on the other hand, feel that the computer security industry can learn from and work with hackers (Taylor, 1999: 93).

Taylor, and those he interviewed, presents three arguments with respect to laws and regulations; all stress that those laws that pass must be able to adapt quickly. The first argument is that laws will be ineffective in eliminating hacking. Next, many hackers believe that companies providing computer hardware and software will hide behind the laws and not fix the known security flaws in their products. Third, that prosecuting hackers may drive them and their skills into the hands of criminal organizations (Taylor, 1999: 124).

Convicted hacker John Draper, who Taylor interviewed via e-mail, supports this view. Draper states that many hackers who serve prison sentences are approached after they are released by embezzlers, scam artists, and other related criminal elements that they met while in prison. They are offered large sums of money to teach automated hacking techniques (Taylor, 1999: 172-173). Such incidents can spread hacking skills to broader elements of society – both white collar and hardened criminals, as well as hate groups, transnational organizations, and terrorist groups. Taylor believes that the pressure to hack for financial gain may rise as hacking techniques become more desirable to traditional criminals (Taylor, 1999: 22). Finally, many "older" generation hackers see the newest hackers as "true computer thugs". Hacking for this group is seen as a way to control their world, as a way of feeding their desires for power, and a way to "learn and abuse for their own gain" (Taylor, 1999: 161-162). Governments at all levels and in all industrialized nations must come to terms with these issues.

2.3. Malicious Hackers

The term “hacker” has evolved over time. Originally, a “hacker” was someone who explored the full range of capabilities of both himself and his computer equipment (Taylor, 1999: xii) –a tinkerer trying to learn about an unfamiliar system or to improve known ones (McClure, *et. al* 1999: xxv). The original meaning of hacker is often now associated with the term “cyberpunk”(Taylor, 1999: xv). Largely due to portrayals in the media, a "hacker" is now perceived as someone who intrudes upon another's computer systems to further his or her own, possibly criminal, ends (Taylor, 1999: xi). This mentality was originally described by the term “cracker”, a term generally no longer in vogue (McClure, *et. al* 1999: xxv). For the purpose of this research, the term “hacker” will be used to describe an individual who maliciously, or without authorization, breaks in to a computer system, whether to gain information or exploit the system in some other fashion.

One type of attack that is of interest to this effort is Denial of Service (DoS) attacks. DoS attacks can be the result of frustration when efforts to break into a system have failed, for the sense of power it can bring, or can be used to carry out a grudge against an organization (McClure, *et. al* 1999: 340-341). McClure also feels that DOS attacks will increase due to tools that allow easy launching of DOS attacks, and the opinion that Windows NT/95/98 is a favorite, and readily available target. This makes DoS a weapon of choice for terrorists, even if skilled hackers do not care, in general, for this type of attack (McClure, *et. al* 1999: 340-341).

2.3.1. Hackers by Taylor

> "Analyzing the computer underground is inherently difficult. It appears as a 'gossamer framework' mixing real-world relationships and the immateriality of cyberspace with the result that its social ties are loose, even by subculture standards" (Taylor, 1999: ix-x)

Taylor sympathetically describes the hacker culture, based in part upon e-mail and in-person interviews from hackers worldwide (Taylor, 1999: ix-x). Changes in society, as a result of the computer revolution, rest on two elements – the rate of technological change, and the fact that the world is increasingly viewed in informational terms (Taylor, 1999: xiv). Taylor sees the dependence upon technology to be the main attribute of cyberculture, with two key parts – the hack and the hacker ethic (Taylor, 1999: 27).

There are three main characteristics to every hack: simplicity, mastery of an aspect of technology, and the illicitness of the act (Taylor, 1999: 15). Anonymity allows the hacker to engage in elaborate role-playing, with limited fear of reprisal (Taylor, 1999: 5). The hacker ethic has evolved over time. Most nonmalicious hackers subscribe to all or portions of a common code (Taylor, 1999: 25). This code involves concepts such as: respect for other's property; the view that information should be free; and, inflicting damage is wrong.

One of the crucial elements is still the curiosity that people have with computer equipment (both hardware and software). The worldwide computer networks allow people from diverse locations to cooperate in explorations of the Internet (Taylor, 1999: 27). This exploration comes with anonymity – the normal cultural associations with race, gender, age, geographic location, or social level do not exist in cyberspace (Taylor, 1999: 30). Common interests, such as technology, transcend geography, culture, and language.

One of the main problems in describing or quantifying computer culture is the secrecy and fluid nature with which its society changes – people changing aliases, tools and techniques, and group associations (Taylor, 1999: 28). The efforts of law enforcement to stop hacking have contributed to secrecy and unwillingness to talk with those interested in describing cyberculture (Taylor, 1999: 29). However, one can state that hacker culture depends upon technology, however technology is defined. Hacker culture exists within the environment of computers, with no real physicality that is comparable to other cultures (Taylor, 1999: 26).

As discusses previously, the term hacker did not originally have the same connotation that it does today. The term was coined in the 1960's to represent the imaginative and unorthodox use of any technology (Taylor, 1999: xi-xii). Original hackers, and nonmalicious hackers today, were looking for the most elegant way to solve a given problem. Hacking was considered a playful, yet highly skilled, academic pursuit (Taylor, 1999: 14). A hack can also be defined as a "quick bit of work", technique without knowledge of how or why it works (Taylor, 1999: 88). This is more in line with today's definition of a "script kiddie". When compared to normal methods of writing computer code, hacking is seen as a more holistic approach, whereas traditional methods are seen as reductionist and fragmented (Taylor, 1999: 88).

Today the term "hacker" is highly contested. Any given definition may serve to establish boundaries between groups. Key elements of most definitions deal with exploration, obsession, ingenuity, and issues of legality (Taylor, 1999: 13-15). Dutch hacker Rop Gongrijp provided the following definition in an interview with Taylor (Taylor, 1999: 17). "...hacking is a frame of mind, a sort of intellectual curiosity that attaches itself to more than one type of technology or technological artefact ...." Hackers were originally tolerated for their expertise, no matter the manner in which it was gained. The information revolution and the commercialization of computers now makes hacking less tolerable (Taylor, 1999: 67).

It becomes an issue of trust – some companies do not believe that hackers have the discipline to strictly follow the rules and keep their innate curiosity in check (Taylor, 1999: 105). In the case of an IO "warrior", this may or may not become an issue. If the hacker can be trusted not to hack systems belonging to friendly nations, and are given "permission" to explore adversary or potential adversary systems, there may be a limited set of "rules" that one wishes the hacker to follow. This relates to the issue of doctrine and its implementation through IO. Should IO be afforded more flexibility in target selection, weapons mix, and operational planning in order to take advantage of its inherent flexibility, speed, and surprise? This issue will be explored more fully in Chapter 3.

Like many who explore hackers, Taylor has found most hackers to be male. Three factors are seen as discouraging women. First is the same set of societal factors that discourage girls from playing with technical toys, math, and science. Second, the masculine environment in the hacking culture, which could be viewed as similar to "locker room" culture, might discourage women. Finally, the issue of gender in language could dissuade some women from participating in hacker culture (Taylor, 1999: 33). Recent efforts to encourage young women to pursue technology, math, and science could change the number of women involved in hacking. Additionally, Taylor believes that the feelings of power conveyed by hacking may appeal to young boys more than to young girls. The desires of boys to explore and the machismo projection of hackers as independent loners may also explain the difference in participation levels. In addition, Taylor feels that the anonymity involved in hacking may allow males, who feel powerless in society, to feel empowered in the computer world (Taylor, 1999: 34, 37-38).

Taylor proposes his own views of hacker motivation, after his discussion of cyberculture. These motivations include compulsive programming (Taylor, 1999: 44), a thirst for knowledge (Taylor, 1999: 46), boredom (Taylor, 1999: 52), a feeling of power (Taylor, 1999: 56), desire for peer recognition within the hacking community (Taylor, 1999: 58), political acts (Taylor, 1999: 60), and rebellion against perceived bureaucracy and authority (Taylor, 1999: 61). The motivations are not mutually exclusive; one or more could be operating at the same time (Taylor, 1999: 46).

Compulsive programming refers to a feeling of addiction; that a hacker must "hack" much as a drug addict must continue to use drugs. The rate of technology change, possibly combined with feelings of addiction, means that hackers must have a high level of commitment in order to stay abreast of technological advances (Taylor, 1999: 49). The urge of curiosity is a similar driving force for hackers, and curiosity in general is what drives technology forward. Taylor, and other authors, sees this as a positive motivation (Chantler, 1996: 78; Taylor, 1999: 50). Hackers are testing the limits of current and developing technology (Taylor, 1999: 51).

Balancing hackers' curiosity is the desire to avoid boredom. This is often associated with younger hackers not challenged by the educational system (Taylor, 1999: 52-53). As a result, they turn to technology to find new puzzles to solve. Knowledge of computers is often not learned in school, but like hacking skills, is self- or peer group-taught (Taylor, 1999: 76). These hackers sometimes stop their illicit pursuits once adequately stimulated by college curricula (Taylor, 1999: 52-53).

Breaking into system may allow a hacker to feel he is "better" than the system administrator, providing a sense of power (Taylor, 1999: 57). There can also be a feeling of "beating the system". This sense of power, combined with a sense of adventure or exploration, may help explain why hacker magazines and websites carry articles on potentially destructive information such as bomb making (Taylor, 1999: 58).

Hacking is also a method of obtaining peer recognition or prestige. Social interaction with other hackers, those who share and understand their interests, can be a key motivation for many hackers (Taylor, 1999: 59). With recognition of past accomplishments and abilities comes access to more information, and potentially an invitation to join a group (Taylor, 1999: 60). Groups pool resources (skills and information) to accomplish more than one hacker can on his own. Recognition within the group can add to the competitive, machismo environment (Taylor, 1999: 60). Group size is often 6 to 7 members, each with specialized skills or areas of expertise (Taylor, 1999: 60).

In addition, hacking can be a form of political protest. For example, the hacker ethic states that all information should be free. Some hackers claim to hack to gain and share information that is being denied to the public (Taylor, 1999: 61-63). In some cases, this can help explain the number of hacking attempts against government organizations. Hacks may also be an anti-establishment statement. Finally, Taylor believes some hacks to be a "blow" against the "dehumanization in the techno-bureaucratic world" (Taylor, 1999: 61-63).

Taylor also explores issues of computing skill and approaches to hacking. Rob Nuata, a Dutch hacker interviewed by Taylor, believes that finding holes in computer security takes either luck or expert skill. "Experts generally know how to crack a system but don't find it challenging, worth the trouble." (Taylor, 1999: 103). Many people fail to take into account the danger of insiders who are intimately familiar with a particular system (Taylor, 1999: 70). Ironically, most incidents highlight known security weaknesses. Hackers have even been criticized for rarely making use of original, unknown security flaws (Taylor, 1999: 71). Some experts suggest that hackers' often unstructured approach could benefit from more structure, something more than just "rattling the doors" (Taylor, 1999: 102). Many hackers, however, have an "instinct for serendipitous discovery", according to Taylor (Taylor, 1999: 73). They sometimes think in ways that system designers would not consider logical, and in so doing, the hackers find ways around roadblocks that would otherwise block their paths.

Hackers often have the time to thoroughly research topics or systems of interest and specialize in narrowly defined specialty areas (Taylor, 1999: 78). This time is rarely available to computer security experts. Chris Goggans, a former hacker and co-founder of computer security firm ComSec Ltd, commented to Taylor via e-mail

> "...I can monitor data on any network in existence, I can obtain root privileges on ANY Sun Microsystems UNIX. If I, a 22 year-old, non-degreed, self-taught individual can do these things, what can a professionally taught, profit motivated individual do?" (Taylor, 1999: 70)

Even if security experts assume previous barriers in a system have been overcome when building layered defenses, total security may not be possible for some systems since "weaknesses cannot always be foreseen" (Taylor, 1999: 73). Statistics on computer security incidents are hard to use as a basis for the level of "crime" involved. Incidents can be under-reported due to companies who do not know that their security has been compromised and due to those who do not want to advertise their vulnerabilities. On the other hand, the exaggeration of incidents by the media, computer security experts, and hackers themselves can lead to over-reporting of incidents (Taylor, 1999: 67-68). Factors that contribute to continued security holes include commercial pressures to ship code quickly, the low status of security in software design, constant updates and expanding networks, exaggerated marketing claims, apathy, and hype (Taylor, 1999: 81-86).

2.3.2. Hacking Exposed by McClure, Scambray, and Kurtz

McClure, Scambray, and Kurtz explain the tools and techniques that hackers use, as well as ways system administrators can thwart hackers' efforts. A basic attack methodology is presented. The skill level of a given hacker determines how faithfully and well they follow these steps (McClure, Stuart, Scambray, Kurtz, 1999: xxvi). The steps in a successful hack are: target acquisition and information gathering; initial access; privilege escalation; covering of tracks; and planting back doors. Since the purpose of this thesis is to profile hackers, not to explain in detail how they accomplish their tasks, not all of these steps will be fully discussed.

Target acquisition often begins with network mapping via ping sweeps (McClure, *et. al*, 1999: 34). This can greatly reduce the target set to be explored, saves time over the course of the hack, and allows the hacker to focus efforts only on "live" hosts. Once a live host has been identified, the hacker tries to identify what system it is on (McClure, *et. al*, 1999: 51-52). Banner grabbing or stack fingerprinting can provide valuable information such as vendor name and version number. Banner grabbing, or banner enumeration, consists of simple tasks such as opening a telnet connection (for UNIX or Windows NT) and pressing enter a few times to see what response the target system provides (McClure, *et. al*, 1999: 70). In many cases, the target system will reply with both an error message and information on the system hardware and software. Stack fingerprinting, which requires a listening port on the target system, is a technology that can determine, with a high degree of accuracy, the components of the target system (McClure, *et. al*, 1999: 52). These efforts aid in vulnerability assessments.

Tools to aid in target identification and information gathering include netcat, Back Orifice, and NetBus. Netcat, often referred to as the "TCP/IP Swiss Army knife", can be extremely successful in hacking NT or UNIX systems (McClure, *et. al*, 1999: 70). It aids in banner grabbing, port scanning, establishing remote backdoors, and running remote shells. Back Orifice is a similar tool that uses UDP ports, and is often not screened out by firewalls (McClure, *et. al*, 1999: 98). Finally, NetBus, which uses TCP ports, is more effective at taking control of remote Windows systems.

Vulnerability mapping is the next step in target acquisition and information gathering. It is a step that script kiddies often skip. Instead, script kiddies tend to throw everything they have at a system (McClure, *et. al*, 1999: 209). This helps explains why many script kiddies do not know how or why an exploit worked. Key points of vulnerability mapping include:

- Network reconnaissance;
- Mapping system attributes to known vulnerabilities and exploits;
- Target acquisition by identifying and selecting key systems; and,
- Enumeration and prioritization of potential points of entry (McClure, *et. al*, 1999: 209).

Once a hacker has taken over a system, they often install a "rootkit" so that they can return again in the future, or pass the capability on to other hackers. These rootkits are often so well hidden that, even if part of the hacker's exploits have been detected and the vulnerabilities corrected, they are never found by system administrators.

Rootkits consist of four tools: trojan programs, back doors, interface sniffers, and system log cleaners (McClure, *et. al*, 1999: 252). A trojan program is one that pretends to perform a useful function, but also performs code in the background without the user's knowledge (McClure, *et. al*, 1999: 132). Often the background code is malicious in nature. A back door is simply a method for the hacker to return undetected in the future, generally through the use of hidden files (McClure, *et. al*, 1999: 438). An interface sniffer captures, interprets, and stores packets traveling in a network for later analysis (McClure, *et. al*, 1999: 253). The sniffer can provide information on any system that the compromised system is connected to, potentially expanding the hacker's power.

One method of gaining information about a system, and also of attacking it, is wardialing. This consists of dialing a large set of phone numbers believed to belong to a target. The goals of wardialing include identifying those numbers attached to computer systems, attempting to break access codes to dial out from the Public Branch Exchange (PBX), or trying to break into systems attached by modems (McClure, *et. al*, 1999: 270-277). This is one danger of cable modems and other internet connection that are "always on" – they are always open to wardialing and ping sweeps by hackers. Much of the general public is unaware of this danger, and the need for home firewalls.

A related attack is the Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack. The goal of a DoS or DDoS attack is to prevent use of a system by bandwidth consumption or resource starvation (McClure, *et. al*, 1999: 344). Many "point and click" tools exist for DOS attacks, making them easy to launch. DOS attacks may be used to force a system reboot so that changes planted by the hacker can take effect, hopefully without the system administrators noticing the changes (McClure, *et. al*, 1999: 340-341). The authors believe that DoS attacks are the last resort of unskilled hackers who are frustrated with a system that thwarts their efforts, or are motivated by personal or political vendettas (McClure, *et. al*, 1999: 340). The simple nature of these attacks leads the authors to state that DoS will be the cyberterrorist's weapon of choice (McClure, *et. al*, 1999: 341). "Many governments have or are in the process of ramping up offensive electronic warfare capabilities that use DoD attacks rather than conventional missiles" (McClure, *et. al*, 1999: 354)

2.3.3. Risk: The Profile of the Computer Hacker by Chantler

Nicholas Chantler, a former head of computer security for the Australian Army, developed a hacker profile based upon his years of work in computer security, as well as interviews and survey of hackers during the development of his doctoral dissertation. The goals of Chantler's dissertation were to conduct an ethnographic study of hackers; to explore how hackers are represented in the press; and to determine the threat or risk hackers pose to society at large (Chantler, 1996: 3). Objectives of the study included a description of the hacker environment; identification of hackers characteristics; a model of how hackers process information; and development of a threat / risk approach that encompasses hacker generation, limitations, and proposed methods of control (Chantler, 1996: 3). Since many of his conclusions are based upon surveys and interviews of those willing to participate in the study, care must be taken in interpreting results since a random sample was not possible (Chantler, 1996: 169).

Chantler identifies three types of people who hack (Chantler, 1996: 13). First are students, who represent 49% of hackers according to Chantler's research of 284 reported events. Next, at 22% are criminals – those subsequently convicted of a crime. Chantler feels they were mainly hacking for monetary gain (Chantler, 1996: 12). The final group, representing 29% of the incidents, were "others". This group contained computer-security specialists, system administrators, law enforcement, journalists and authors.

Chantler participation in underground hacker electronic bulletin-board systems (BBS) lead him to the following conclusions on those who frequented the BBS. First, three groups seem to exist: intelligent and well educated; bright but poorly educated and often on the wrong side of the law; and those that are juvenile and inexperienced (Chantler, 1996: 62). As a whole, the members of BBS had several common attributes:

- A loose hierarchy exists and teams from of between four and seven members (some members with special skills);
- Successful hackers tend to be of above average intelligence, imaginative, curious, and inventive;
- Some members are "loners", many of whom are respected for their ability to think "laterally" and push technology into things it was not designed to do;
- A group language has evolved, consisting of abbreviations, slang, and visual representations of feeling, that overcomes the limitations of communication solely via keyboard;
- All claimed an addiction to computing;
- They believe they can do anything they want;
- Enjoy a sense of power and achievement through the systems they have hacked; and,
- Targets of choice include military, government, and university systems and web sites (Chantler, 1996: 62).

Chantler spends some time exploring issues of how and why hackers begin to hack. The home environment is seen as a key factor (Chantler, 1996: 78). He feels the high number of juvenile hackers in single-parent homes, often looking after younger siblings, creates an environment that pushes hackers to "bury themselves in the PC" (Chantler, 1996: 78). Via the Internet, these hackers find friendship and support from others in similar situations. The home situation, especially in cases of dislike of step parents, may lead to attitudes of contempt and arrogance toward "the system", resulting in little respect for laws regarding illegal hacking (Chantler, 1996: 78).

It is interesting that Chantler places such emphasis on answers to the home life questions. Only 41% of the respondents replied that their home environment was sad, boring, frustrating, or dull. Chantler feels this supports his theory that unhappy home life may lead people to hacking (Chantler, 1996: 95). However, 59% of respondents felt their home life was happy and rich.

Chantler developed a computer-based survey, to which he received 164 replies he felt were valid (of 191 total responses). The survey consisted of questions regarding personal details, when hacking activities began, home life, school / university experiences, work, computing, and hacking (Chantler, 1996: 83).

Most hackers that responded were male, although 5% were female. Real names were provided by 67% of the respondents, but all provided their "handles" (the name they go by in the hacking community). Their ages were between 11 and 46, with the majority in the 18-24 year range (Chantler, 1996: 83-84).

Most respondents began hacking within months of owning a PC, with an age range of 11 to 26 years of age (Chantler, 1996: 85). Many listed a sense of power or control provided by the computer as a reason for beginning to hack (Chantler, 1996: 86). Discussions or demonstrations by peers convinced 40% of the respondents to hack (Chantler, 1996: 86). On average, respondents were familiar with three operating systems, although nine respondents were only familiar with one system (Chantler, 1996: 91). UNIX and DOS were the best-known systems, and could represent the most likely targets (Chantler, 1996: 91).

When it comes to targeting of systems, the majority (78%) did not pursue specific targets (Chantler, 1996: 87). They predominately went to sites that had previously been exploited. Those that did target particular sites chose their targets based on the level of challenge, particular interests in technology inherent in the system or contained in it, or the thrill or "excitement" value of the site (Chantler, 1996: 87).

Chantler asked if threat of detection or prosecution inhibited hackers. Only 73% of the respondents answered the question. One was afraid of a criminal record, but the rest did not feel threatened by existing laws (Chantler, 1996: 88). Current legislation was viewed as ineffective by 91% of the respondents.

The motivations listed by survey respondents corresponded with those previously discussed: addiction, freedom, knowledge, recognition, self-gratification, pleasure, challenge, friendship, excitement, profit, sabotage, espionage (obtain access to restricted information), theft, and vengeance (Chantler, 1996: 89). Chantler found that 49% of the reasons that the respondents hacked was for challenge, knowledge, and pleasure. Recognition, excitement, and friendship accounted for 24% of the motivations. These motivations were seen as "positive" or "harmless" (Chantler, 1996: 89).

Over 70% of the respondents wish to work in the computing industry when the finish school. An additional 15% are interesting in investigation, intelligence, security, and police work (Chantler, 1996: 107). This might mean that a potentially large work force would be available to nations or other organizations looking for the hacker's unique skills over the next few years. Of interest to those that might hire hackers, 41% stated that they do not use computers to hack from work; 15% stated that they did (Chantler, 1996: 108). This second group could pose an insider threat.

Overall, Chantler sees hackers as a very valuable resource at the forefront of computer technology (Chantler, 1996: 168). Their self-motivation and devotion to hacking could make them an important asset to governments or corporations that require high levels of computer skills. The only drawbacks are limiting a hacker's curiosity about forbidden systems, and the small (according to Chantler) number of hackers without the ethical background to determine right from wrong (Chantler, 1996: 168).

2.4. Profiling, the Criminal Mentality, and Psychology

Most published profiling to date is of the criminal mentality, more specifically, that of the violent criminal (Godwin, 2000: iii). This type of mental model may not apply in totality to the classes of hackers relevant to this research. The national or religious activist does not have the same goals and motivations as the serial killer; however, some of the basic drives and compulsions may prove similar.

2.4.1. Hunting Serial Predators

The primary reference on profiling, Godwin's Hunting Serial Predators, was chosen due to its basis in multivariate data analysis. The author seeks three main goals in his classification scheme of profiling: reliability, ease of interpretation and use, and validity for its intended uses (Godwin, 2000: xvii). As he discusses in his Prologue, many efforts at profiling behavior are based in deductive reasoning. Godwin defines deductive reasoning as assuming facts to be self-evident, and then using these facts, and past experience, to make conclusions that are then, themselves, stated as facts (Godwin, 2000: iii). The assumptions often have a cultural bias based upon the views and background of the investigator (Godwin, 2000: xviii). The FBI considers their approach to serial killer profiling to be inductive, meaning it is an empirical framework based upon formal analysis, since interviews with known serial killers are used as a basis for their profiles. Godwin considers the FBI's efforts as deductive, since he feels the profiles have not been empirically analyzed or systematically organized. Godwin used data from past crime scenes across many databases as a basis for what he considers a truly inductive approach to profiling (Godwin, 2000: viii). The key questions he seeks to answer in his research are also applicable to a hacker mentality model, specifically:

1. Does a specific serial killer show common behavior across his victims;
2. Are their unique types of serial killers;
3. Do a given type have common underlying background characteristics; and finally,
4. Is there consistency across time in both behaviors and killers (Godwin, 2000: ix)?

Godwin feels that the FBI's organized and disorganized classifications of serial killers is faulty for several reasons (Godwin, 2000: 12). First, the original interviews with jailed serial offenders were unstructured. Second, no analysis of the offenders' background information has been published. Additionally, there is no literature to explain the difference between organized and disorganized offenders, although Godwin feels it is based upon theories of aggression and personality. Finally, an offender that does not fit into either type is not addressed.

The underlying methodology of Godwin's approach is the Thematic Facet Model, where a facet is defined as a categorical framework for a group of data (Godwin, 2000: 29). Facet theory is based upon a geometric representation of complex relationships within a set of observations. Multivariate hypotheses are combined into an empirical procedure for their validation. Multivariate statistical procedures are used to determine underlying relationships within the data. The three types of facet structures (background, domain, and range or content facets) are used to explore individual differences (background) on common areas. Range facets are then possible reactions to a specific stimulus from the domain facet, allowing for different reactions by an individual at different times (Godwin, 2000: 30).

This appears to be a fruitful method of explaining individual differences of hackers from a common group. Each facet contains all of the elements that describe variations in that facet. Similar to decision theory, facets and facet elements should be mutually exclusive. Mutual exclusivity of variables is another of Godwin's criticisms of FBI profiling (Godwin, 2000: 30).

Key facets in the model are Behavioral Organization and Attachment (Godwin, 2000: 32 - 42). The behavioral facet of Godwin's model is further divided into two elements – affect (feelings and emotions) and cognition (beliefs and rational behavior) (Godwin, 2000: 33). The Attachment facet is divided into victim as object and victim as vehicle elements (Godwin, 2000: 40). These two elements are a relation of how the offender sees his interaction with the victim; a similar construct might be computer system as end or computer system as means to another (non-computer based) end.

The methodology used by Godwin in his data analysis was Smallest Space Analysis (SSA), a subset of Nonmetric Multivariate Analysis (Godwin, 2000: 58). The data was obtained from a variety of sources such as eyewitness accounts, crime scene evidence, telephone conversations with the killer, and medical reports on the victims (Godwin, 2000: 53). SSA seeks to determine whether a hypothesized order within a set of data is organized in such a manner that the structure can be tested. Similar to cluster analysis, SSA postulates that related variables will be near each other in conceptual space. An added advantage of SSA is that "empty" space between variable points in the solution region may point to additional variables that are needed but not currently included, since they are close to the current variables in conceptual space (Godwin, 2000: 59). SSA can handle data that is qualitative, quantitative, or both. It is considered robust for categorical, ratio level, discrete or continuous distributions, and numerical data (Godwin, 2000: 58).

Evaluation of individuals within the multivariate data structure is conducted using Partial Order Scalogram Analysis (POSA) (Godwin, 2000: 59). POSA postulates that individuals and attributes may be ordered solely in the dimensions of type and degree. Godwin's overall goal in data analysis was to explain how serial killers relate to their victims and other members of the serial killer group. One of the chief advantages of the facet approach to profiling is the ability to show relationships between variables before, rather than after, the fact (Godwin, 2000: 60).

Finally, as in other profiling approaches, Godwin seeks to model crime scene behavior and background characteristics of serial killers. This is an effort to tie certain aspects in a killer's history, such as marital status and education level to types of serial killers (Godwin, 2000: 194); in the case of the FBI's model, this would be either organized or disorganized. Using the four elements under his two facets, Godwin examines whether there are any differences between killers' characteristics (Godwin, 2000: 194). Total scores for specific crime scene action were summed across an early, middle, and later victim for each offender. These scores were combined into a matrix with scores for each facet element and with scores for background characteristics. POSA was then used to evaluate the relationship between behavior and background variables (Godwin, 2000: 195).

The results showed a mixed ability to predict facets of a killer based solely upon crime scene behavior. In some cases, a single behavior was useful in predicting a background characteristic, in other cases either more behaviors were required for prediction, or no set of behaviors adequately predicted background characteristics (Godwin, 2000: 225). In the case of profiling computer hackers, there may be more difficulty in determining which incidents belong to the same hacker.

2.4.2. Offender Profiling:

This work by Jackson and Beckerian is a compendium of inputs from the US and several European countries. They begin with a definition of profile analysis, also known as offender profiling, psychological profiling, criminal profiling, and criminal personality profiling (Jackson and Beckerian, 1997:2). TREVI, a European initiative to share police information, defines profiling as "attempting to produce a description of the perpetrator(s) of a criminal offense on the basis of analysis of characteristics of the incident" (Jackson and Beckerian, 1997: 2). Tools for profiling include clinical experience, statistical analysis of offender databases, and experimental research, all to answer the questions: what happened at the crime scene, what type of person would most likely have committed the crime, and what are the most likely personality characteristics of that person (Jackson and Beckerian, 1997: 3). The equivalent questions in dealing with computer hackers are: what happened during the incident, what type of hacker is most likely to have committed the incident, and what are the most likely characteristics of this person or group.

Similarly, according to Jackson and Beckerian, the FBI's process for profiling serial killers involves four stages: data assimilation from all sources; crime classification (type of crime); crime reconstruction to generate hypotheses about victim's actions, the sequence of the crime, and the *modus operandi* of the offender; and, finally, profile generation to include demographic and physical elements, behavioral habits, and personality dynamics of the offender (Jackson and Beckerian, 1997: 4). The profile tries to provide an idea of the offender's age range, race, possible job skills, marital status, socioeconomic status, education level and degree of intellectual abilities, arrest history, military background, family characteristics, habits and social interests, personality characteristics, and suggested techniques for interviewing (Jackson and Beckerian, 1997: 5). Of specific note for this research effort, offenses most suitable to profiling are those where the behavior at the crime scene suggest important details about the offender (Jackson and Beckerian, 1997: 5). Again, the FBI approach is criticized for the small data set used in its creation, the dichotomy between the two classes of offenders, and the lack of published research to support their methods (Jackson and Beckerian, 1997: 6).

Underlying clinical (mental illness) and developmental (developed in response to intrinsic personal needs and life experiences) issues are often clearly seen in violent crimes (Jackson and Beckerian, 1997: 10). It is conjectured that these issues would not be as applicable to the profile of a hacker from a structured group. It may be applicable to script kiddies or other individuals not affiliated with a structured or semi-structured group.

One of the areas of the profile is an idea of the type of person that committed the crime – their personality. Personality is defined as those aspects that are relatively enduring characteristics of the person over both time and space, those characteristics which taken as a whole are unique to the individual, and finally those characteristics that suggest the person's thoughts, attitudes, and behavior (Jackson and Beckerian, 1997: 44). The authors are not concerned with the competing theories to explain personality, believing that the different theories are desirable. Different theories can explain a given situation in different ways, some being more applicable to the given situation (Jackson and Beckerian, 1997: 44 - 45).

The five different frameworks of personality theory outlined by these authors are psychoanalytic / dynamic, learning theory, dispositional / trait theory, humanist / cognitive, and alternative / Eastern (Jackson and Beckerian, 1997: 45). When using personality theory on a specific case, one begins with a synthesis of data on the case, then key issues and points are identified, and then the profiler selects a specific framework or personality theory that best suits the case. This theory is next applied to the specific data gathered, and finally the individual profile is developed (Jackson and Beckerian, 1997: 46).

The framework selected must meet two criteria – it must offer the best chance of providing insight into the offender's personality, and offer the most benefit to the investigation (Jackson and Beckerian, 1997: 46). Three extortion cases are used to illustrate this idea. Of most interest is case 2, one of extortion against a supermarket chain in Europe (Jackson and Beckerian, 1997: 52 - 56). The offenders were coherent in their plans, seemed to be of high intelligence and not subject to reality distortion. The plan used was very involved, showing a high degree of knowledge about the area and any potential police actions. The offenders' actions supported a cognitive – social learning theory, specifically, that of Bandura.

Bandura's theory of motivation was chosen based upon the clarity of the offenders' plan, the meticulous way in which it was executed, absence of an affective tone, strong focus on personal gain without the need to justify the actions, and the coherent structure and design (Jackson and Beckerian, 1997: 53). A key aspect of Bandura's theory is that different individuals can have different reactions to the same stimuli – both environment and the individual shape personality (Jackson and Beckerian, 1997: 54). In this case, the profile accurately predicted that the offenders were hardened criminals, that a team was involved, as well as providing clues to whether they would carry out their threats, to their personal history, and to their familiarity with the area involved.

Jackson and Beckerian commented on an effort by Aitken to consolidate data from several sources in the United Kingdom (UK). Databases in the UK were studied to see whether a predictive model of an individual offender could be gleaned from details of the crime (Jackson and Beckerian, 1997: 102). The study found potential for developing such a model, but also found the effort was hampered by such problems as inconsistent coding across source databases, and data sets that were too small. There were also problems with past efforts where inappropriate statistical analysis was used, and with methods of testing the model's reliability (Jackson and Beckerian, 1997: 102). Aitken's study found a trade-off must be made between reliability of the model and the detail of the predictions. Simultaneously predicting several offender characteristics was not possible due to the small data set (320 offenders). He did find that combining the expertise of an experienced detective with the database provided a simple model that could predict several characteristics with an acceptable level of reliability (Jackson and Beckerian, 1997: 103). He believes better predictions to be possible as large data sets specific to the purpose are developed. The results of the study point to the potential benefit in standardized collection of data into shared databases that could best address the characterization of hackers and analysis of their actions.

2.4.3. Psychological Bases of Motivation-

Freud, among other psychologists, suggests that individuals often do not know all that motivates their behavior (Arkes, 1982: 3). Unlike behavior, these motivations are not directly observable. Others suggest that environment is the major influence over behavior. Motivation is defined as "the processes that influence the arousal, strength, or direction of behavior"(Arkes, 1982: 3), and therefore understanding motivation is a key beginning to understand and predict behavior. Arkes points out that both learning and motivation affect behavior, but that learning is the semi-permanent behavioral change that is a direct result of experience (Arkes, 1982: 4). Both learning and motivation affect an individual's current behavior, but in different ways. Motivations are often of shorter duration of influence than learning, since motivations move a person toward achievement of a goal. Motivations occur at many levels – physiological (hunger and thirst), contemporary (social interactions and task characteristics), or past experiences as they may explain motivations (Arkes, 1982: 5). Many types of theories exist to explain different aspects of motivation, yet no overarching theory exists.

Two broad approaches to psychological theory are clinical and experimental. The clinical approach is based upon observations outside of a laboratory, in a natural setting. In this manner, the environment of the subject is not altered by the observation (Arkes, 1982: 7). Since these observations are not as controlled as those of an experimental approach, the results are less exact and the overall process is less systematic. On the other hand, experimental approaches to motivation theories are based upon laboratory experimentation and concepts that can be directly observed (Arkes, 1982: 6). As such, care must be exercised in extending laboratory results to real-life situations.

Several key theorists have contributed concepts that might apply to developing a hacker profile. Specific examples are Maslow's concept of self-actualization, Berlyne's optimal level of stimulation, Rotter and Bandura's social environment and cognitive variables, and Lewin's "field theory". A final area of study is achievement motivation.

Maslow:

Maslow's theory of self-actualization, as discussed by Arkes, is a clinical approach to motivation, and is humanistic in philosophy (Arkes, 1982: 108). It and other humanistic approaches look at motivation as the effort of an individual to achieve his or her full potential, self-actualization. Two key aspects of this approach are that motives affect behavior in a straightforward way, and that this need for self-actualization is innate and unlearned. As a clinical approach, Maslow's hierarchy of needs (the primary humanistic approach to motivation) relies upon observations and their interpretations, not upon experimental results (Arkes, 1982: 111). The hierarchy of needs is based upon a system of motives that can influence behavior. Those on lower tiers must be met before the individual moves on to higher levels (Arkes, 1982: 123).

The levels progress from survival of the person to self-actualization in five stages: physiological needs, safety needs, belongingness and love needs, esteem needs, and finally self-actualization needs (Arkes, 1982: 125). As lower level needs are satisfied, the demands of the next level become dominant over behavior. Safety needs such as security, stability, and a need for order can be seen in views towards religion, philosophy, and other ideologies an individual may hold (Arkes, 1982: 125). Esteem needs, the need for status, respect, and recognition, may be a key area of focus for a hacker profile, based upon the degree of technical proficiency needed.

This may also be true for the highest level of the hierarchy – self-actualization. This highest level of motivations is where Maslow's theory shows the greatest degree of individual expression, as different people are drawn toward different activities (Arkes, 1982: 127). All of the levels of the hierarchy are motivated to overcome a deficiency (such as in safety), except for self-actualization, which is a growth motivation beyond satisfaction of needs.

Berlyne:

Berlyne, according to Arkes, is the prominent theorist of an inherent optimal level of stimulation. His theory is based upon an experimental approach (Arkes, 1982: 177). Basically, every individual has a certain minimum level of stimulation that they require from their environment. His theory states that people want to optimize their "arousal level" based upon stimuli that have properties such as surprise, novelty, or complexity. Everyone has his or her own individual optimal level of arousal potential (Arkes, 1982: 178). Preferences for a stimulus drop off in a bell-shaped curve from the optimal level for all but the individuals who prefer the highest and lowest levels of stimulation.

Of practical application, optimal level theories also include the idea that a stimulus will become less arousing if it is repeated often (Arkes, 1982: 179). It then follows that a hacker who can readily break into a given system, or into multiple systems with the same tool, may become bored with that system or tool over time and move on to something new. An important note is that stimuli that were initially higher than a person's optimal level actually become more popular upon repeated exposure, as they move toward the optimal level, and then drop below the optimal level with even more exposure.

Finally, organizational principles or coding schemes can create a unified picture of a stimulus, thereby reducing its perceived level of complexity (Arkes, 1982: 181). Basically, experience with a stimulus reduces its novelty and provides a framework for experiencing the stimulus. This theory has ties to environmental research – how the environment itself influences behavior (Arkes, 1982: 188).

Rotter and Bandera:

Arkes also discusses the theory of social learning and cognitive perspectives. Developed by Rotter and Bandera, this approach combines aspects of both clinical and experimental approaches. Its concepts of observational learning and vicarious reinforcement have been used to explain such things as the potential ties between children's aggressive behavior and violence on television (Arkes, 1982: 197). For a social learning theorist, the processing by an individual of information concerning motivational variables is the critical determining factor for behavior.

Rotter proposes an expectancy-value theory for social learning. This theory specifically focuses on complex social interactions and behavior. It readily provides a heuristic framework for personality assessment, and it emphasizes the individual aspects of motivation and learning (Arkes, 1982: 204). However, its experimental basis limits its real-world applications.

Bandura's social learning theory also focuses on complex social interactions. His theory includes the idea of symbolic rewards, that someone need not be specifically rewarded or punished in order for learning to occur (Arkes, 1982: 212). An individual can reinforce and motivate his or her own behavior based upon observation of others. Bandura's theory is largely descriptive rather than explanatory, which is a criticism from a scientific perspective (Arkes, 1982: 212), but may make it better suited for the purposes of modeling a hacker. A more substantive criticism is the theory's ability to explain behavior in great detail after the fact by overuse of cognitive mediating variables (Arkes, 1982: 225). Additional variables, not originally part of the study, are generated until the observed data is best explained.

Lewin:

Lewin's field theory states that, according to Arkes, behavior is based both upon the individual and the environment (Arkes, 1982: 228). Thus, two people exposed to the same environment can perceive the same situation in two different ways.

Behavior is directed in one of four ways. The basic direction is oriented from the current "region" (i.e. activity) toward the same activity, toward a nearby (in physical or psychological space) region, away from the current region but not toward a specific new region (i.e. just getting away from something seen as unpleasant), or away from a remote region. Motivational constructs are the forces that cause a person to move in one of these four directions (Arkes, 1982: 230).

Primary criticisms of Lewin's approach to motivational theory are the lack of operational definitions and its inability to make predictions. In addition, field theory does not account well for individual differences, even though it is based upon the idea that both the individual and the environment affect behavior (Arkes, 1982: 248 – 249). However, Lewin was one of the first to introduce strong cognitive aspects to a theory of motivation (Arkes, 1982: 250).

Achievement Motivation:

Lewin's field theory influenced achievement theory, which is solely concerned with motivation. It is both controversial and practical in nature, and has shown wide applicability to a diverse range of topics, such as gender and racial differences in motivation (Arkes, 1982: 252). Its underlying idea is an individual's underlying need to achieve success and to avoid failure (Arkes, 1982: 256). An interesting notion is that if the need for achievement can predict the behavior of individuals, perhaps it can also predict the behavior of groups of individuals. This general approach has been successfully applied in hindsight to British economic growth over a 350-year period (Arkes, 1982: 277).

The assessment of the need to achieve is based upon the Thematic Apperception Test (TAT), where an individual creates a story around an ambiguous picture (Arkes, 1982: 252). In the case of societal trends in achievement, writings about the same general topics were compared across many years. Some experts question the validity of the TAT to measure motivation (Arkes, 1982: 286), based upon studies where need for achievement does not predict well a given measure of performance. Atkinson, one of the developers of achievement theory, defends the theory with Yerkes/Dodson's law (Arkes, 1982: 287). This states that people with a low need for achievement do better on hard tasks, while people with a high need for achievement perform better on an easy task.

2.5. Foreign Actors: Governments, Terrorists, Transnational Criminal Organizations

State sponsorship of terrorist organizations is seen as waning (Lesser, et. al, 1999: 130). This has lead to an increase in the level of violence used by terrorists that are no longer constrained by conservative state sponsors, but rather are less constrained by criminal organizations or wealthy nonstate sponsors (Lesser, et. al, 1999: 131). A key challenge for the US is finding ways to respond to IW attacks by individuals, nonstate groups, and terrorist organizations when these actions are launched within the borders of states with which we are not at war (Lesser, et. al, 1999: 131). Deterrence and response must focus on key nodes in terrorist networks, yet the distributed nature of the terrorist organizations and methods of secure communication can make them hard to identify (Lesser, et. al, 1999: 142).

2.6. Outsourcing and the Rise of IO Mercenaries

On the subject of mercenaries, Machiavelli warns the prince "They have no love or other motive to keep them in the field beyond a trifling wage, which is not enough to make them ready to die for you" (Machiavelli, 1962: 72). A mercenary's loyalty is not to those that hired him, but to himself. Ultimately, without stronger ties of loyalty to the hiring organization, money is not enough to ensure performance during times of war. Mercenaries, then, may provide outstanding service during the safety of peaceful times, but leave or demand higher pay during the dangerous times of war or conflict.

In the case of IO, this concept may be altered. The advantage of IO is the ability to attack any target from the safety of an anonymous location. For this reason, there may be a growth in the number of IO warriors who are not active duty members of a nation's military. The advantage to the military is a highly skilled workforce that is "bought" rather than "trained". A contractor's salary is not limited by standard military wages and benefits, but only by the budget the military can spend on purchasing offensive IO capability.

Military contractors have a different motivation from military members. Salary is a primary motivator for their service. Consequently, they can be loosely defined as mercenaries. The contractor's salary will be based upon skills, demand, risk, and the level of competition present in the marketplace (Lavadour, 2001: 59). Terrorist and criminal organizations may also begin to make use of "hired" hacking talent rather than trying to "grow" their own expertise. This can impact profiles of malicious hackers belonging to nation states.

According to some mercenaries, many who prefer to be called "contract soldiers", they are businessmen first (African Business, 1997). "We have highly specialized, intensely trained and thoroughly disciplined teams able to deliver a unique service: security. ... We go where we are wanted and where people can pay our fees." (African Business, 1997) Many of these groups are looking for a certain amount of respectability; for example, they say they will only work for legitimate governments. Some will also work for multinational corporations. They freely admit that they wish to earn large profits, which may involve such items as mining concessions (African Business, 1997).

The Geneva Convention bans the use of mercenaries, but "the distinction between soldiers of fortune and private security firms is blurred" (African Business, 1997). The many small wars that have grown since the fall of the Soviet Union, especially in Africa, contributes to the growing acceptance of private security firms. These forces may be perceived as more "neutral" than a UN peacekeeping force. They may also prove cheaper and more effective (African Business, 1997).

Their leadership often contains former high-ranking military and national security advisors from many nations (African Business, 1997). Services provided by these contract soldier firms have grown more specialized. Many of the firms focus on protection, security, and training. In some cases they may actually participate in combat (African Business, 1997). An expansion into IW will probably occur in the near future, if it has not already happened.

2.7. Statistical Analysis Techniques

In addition to the data analysis techniques mentioned by Godwin in his approach to profiling serial killers (Godwin, 2000), other techniques in the areas of multivariate statistics can provide valuable insight into the specific evidence gained from a substantiated computer incident. Additionally, basic linear regression could also provide insight into the relationships within the data. Where data is available, these techniques will be utilized in building the malicious hacker framework.

2.7.1. Linear Regression

Linear regression utilizes the relationship between variables to better predict a single dependent variable. The independent variables used to predict the dependent variable can be quantitative or qualitative (Neter, Kutner, Nachtsheim, and Wasserman, 1996: 455). Predictor variables are sought that explain the dependent variable better than the grand average (Neter, *et. al*, 1996: 217). The basic model is of the form:

$$Y_i = \beta_0 + \beta_1 X_{i1} + \beta_2 X_{i2} + \varepsilon_i$$

Equation 2-1 Linear Regression Model

The expected value of the error term (ε_i) is assumed to be zero, and the error terms are assumed to be independent and to have constant variance (Neter, *et. al*, 1996: 29, 218). β_0 is the intercept of the regression plane if the range of X_1 and X_2 both include zero. β_1 represents the change in mean response per unit increase in X_1 when X_2 is held constant; a similar interpretation holds for β_2 (Neter, *et. al*, 1996: 218-219). Interaction terms may also exist in the model (Neter, *et. al*, 1996: 308). The Y_i are assumed to be independent random variables, also with constant variance (Neter, *et. al*, 1996: 29). Finally, significance tests exist to determine the how much of the variability in the dependent variable is explained by each of the independent variables or interaction terms. This determines which variables should be in the model, in that they add to the prediction of Y given values for all of the X_i in the model (Neter, *et. al*, 1996: 228).

2.7.2. Cluster Analysis

When presented with data from unknown populations, cluster analysis seeks to group the data into mutually exclusive, homogeneous clusters or groups (Mardia, 1994: 360). A group is homogeneous if members of the group are close to each other, but differ significantly from members of other groups. Cluster analysis can either present a condensation of the data, where the analysis is for descriptive purposes, or can support a model of populations (Mardia, 1994: 360-361). The technique can support single- or multi-sample situations (Mardia, 1994: 360-361). Cluster analysis can also support hierarchical methods of grouping, an example of which is nearest neighbor grouping (Mardia, 1994: 369-370).

The "distance" between groups can be defined in many ways. To be an acceptable distance measure, it must have the properties of symmetry, non-negativity, and identification mark (this distance between a point and itself is zero); a distance may also have the desirable properties of definiteness and meeting the triangle inequality (Mardia, 1994: 376). Examples of acceptable distance measures for quantitative data are Euclidean, Karl Pearson, and Mahalanobis distances (Mardia, 1994: 376-377). Euclidean and Mahalanobis distances are also suitable for qualitative data (Mardia, 1994: 377-378). Data from hacking incidents would contain both quantitative and qualitative data.

2.7.3. Discriminant Analysis

Discriminant Analysis seeks to allocate an individual, with as few mistakes as possible, to a specific group based upon data about the individual (Mardia, 1994: 300). Populations can either be known, with parameters that must be estimated, or unknown (Mardia, 1994: 301).

In the case of known populations, an individual is assigned to the group based upon the highest likelihood of membership (Mardia, 1994: 301). If there is prior information about which population an individual is from, the information can be incorporated in a Bayesian discriminant rule (Mardia, 1994: 304). A Bayesian approach can also be useful when dealing with small data sets (Mardia, 1994: 316).

When the populations underlying the data are unknown, Fisher's Linear Discriminant Function can provide a way to differentiate between them (Mardia, 1994: 318). This is done by finding a linear function that maximizes the ratio of between-groups sums of squares to within-group sums of squares. It is then easier to differentiate between groups when the between-groups sums of squares if large compared to that within-groups (Mardia, 1994: 319).

2.7.4. Factor Analysis

Factor analysis seeks a small number of underlying factors to explain the underlying correlation of a large set of variables (Mardia, 1994: 255). Since these factors are not directly observable, factor analysis is well suited to the area of psychology. In fact, psychologists originally developed the concept (Mardia, 1994: 255). Maximum likelihood estimation and principal factor analysis (similar to principal component analysis) are the two primary methods used (Mardia, 1994: 255).

In factor analysis, a mean and a sample covariance matrix for a data set is obtained. One then seeks to determine if, for sample covariance greater than zero, a factor model can explain the data better than the covariance matrix (Mardia, 1994: 258-259). In maximum likelihood estimation, the underlying data is assumed normally distributed, the true mean is estimated by the sample mean, and the likelihood of the model is maximized (Mardia, 1994: 263).

An advantage of this tool is that it allows a goodness of fit test for the factors that are chosen (Mardia, 1994: 267). Principal factor analysis assumes all of the factors are uncorrelated (Mardia, 1994: 256). Without these assumptions, and that of a well-defined model, principal factor analysis can result in specious answers (Mardia, 1994: 275).

2.7.5. Canonical Correlation

Canonical correlation partitions the variables of interest into two groups, **x** and **y**. The goal is then to find linear combinations of $\eta = \mathbf{a}'\mathbf{x}$ and $\varphi = \mathbf{b}'\mathbf{y}$ that have the highest possible correlation (Mardia, Kent, and Bibby, 1994: 281). The result is insight into the relationships between the two groups of variables. Since canonical correlation places the fewest restriction on the types of data it uses, some researchers feel the results are of lower quality and less interpretable than other techniques (Hair, Anderson, Tatham, and Black, 1992: 194-195). Canonical correlation is similar to principle component analysis, in that it looks at interrelationships. However, canonical correlation focuses on between group relationships, whereas principal component analysis focuses on within group relationships.

Canonical correlation can also be seen as an extension of linear or nonlinear regression, where more than one dependent variable is being predicted (Mardia, *et. al*, 1994, 281). The group **a'x** would be the best predictor of **y**, and **b'y** the most predictable criterion (Mardia, *et. al*, 1994, 281). However, unlike regression, which assumes causal asymmetry (**x** causes **y**, **y** does not cause **x**), canonical correlation treats both **x** and **y** symmetrically (Mardia, *et. al*, 1994, 281). Additionally, as with regression, canonical analysis does support the use of qualitative data in addition to quantitative data (Mardia, *et. al*, 1994, 290). Finally, canonical correlation does provide significance tests for the correlation coefficients that are developed (Hair, *et. al*, 1992: 198).

All of these multivariate techniques show promise in helping to profile hackers. Unfortunately, they also require a large quantity of data; data that may not currently be available for the specific group of interest.

2.8. Models and Frameworks

2.8.1. Introduction

During the course of research into characterizing hackers, several different types of models were explored. The following presents an overview of each of the most promising model types. More detail on the model selected, Ishikawa diagrams, is provided in Chapter 3.

The key characteristics desired in a model were:

- A descriptive framework;
- A framework that can consider many aspects, such as personality and motivation;
- An estimation of underlying preference functions;
- Ability to use observed and unobserved data;
- Robustness for small sample sizes; and,
- No formal experimental process required.

2.8.2. Value Focused Thinking (VFT)

A few of the past AFIT research efforts that relate to a multi-objective value model and the area of IO are Capt. Rob Renfro's study Modeling Individual Behavior, Capt. Todd Hamill's thesis Modeling Information Assurance: A Value Focused Thinking Approach (AFIT-GOR-ENS-00M-15), and 1LT Philip M. Kerchner Jr.'s thesis Value-Focused Thinking Approach to Psychological Operations (AFIT/GOR/ENS/99M-07). These two efforts applied Multiobjective Decision Analysis frameworks to complex problems in computer systems or psychological operations, both of which have a bearing on this effort. Hamill and Kerchner both used Multiobjective Value Hierarchy theory as the basis for their decision models (Hamill, 2000; Kerchner, 1999). In the case of Kerchner's Psychological Operations hierarchy, one could even state that structured IW attacks would have the same fundamental objective – to modify the attitudes and behavior of opponents (Kerchner, 1999: 3-3).

Value focused models were developed from the viewpoint that a person's underlying values are what should guide their decisions, and therefore their actions (Kirkwood, 1997: 3). Focusing a model on the decision maker's values aids in the evaluation of complex decisions by determining what is desired and then deciding how best to achieve it (Kirkwood, 1997: 11). Multiobjective models then take into account competing objectives that must be traded off to find the best decision (Kirkwood, 1997: 1).

Unfortunately for this effort, the types of "decision makers" one would interview are members of the national and transnational groups to be profiled. While some information about the desires and values of these groups could be gleaned from open information sources, it is doubtful that short to moderate length interviews of these people, if even possible, would truly represent their underlying values. Verification of the model developed would also then be open to discussion of the correctness of the "values" derived form the information sources. Air Force Red Team members, or other comparable groups could be suitable as substitutes for a national, doctrinal group. VFT has been used previously to explore behavior, such as Renfro's basic profile (Renfro, 2000), however its benefits without interviews of the desired group members is an open question.

2.8.3. Item Response Theory (IRT) and Latent Trait Theory

These two model classes, though begun as separate psychological modeling approaches, grew into one common approach with the advent of computing power that could support the use of the models (Weiss, 1983: xiii, 4). Mathematical models are used to explore the functional relationships between observable variables and underlying (latent) trait constructs that are hypothesized to influence the observed variables (Weiss, 1983: 1). The model is then composed of a stimulus, response, and a hypothesized relationship between the response and the trait of interest (Weiss, 1983: 1). The traits explored are often a subject's ability, such as strength or mental aptitude.

The Item Response Theory (IRT) model specifies a probabilistic relationship between an observed response on a test question and the individual's level on that trait (Weiss, 1983: 9). IRT theories were developed to address specific problems in psychology, education, and other social sciences (Hulin, Drasgow, and Parsons, 1983: 14).

In general, the term “item” refers to a specific unit of observation (i.e. test question), “test’ refers to a collection of items, and “trait” refers to the latent (unobserved) characteristic of a test subject (Hulin, *et. al*, 1983: 15).

If the characteristics of the stimulus are known (i.e. how well a specific test question describes a particular skill or aptitude or the question’s difficulty level), then the model can be used to estimate the latent (unobservable) trait level of a subject based upon his or her responses (Weiss, 1983: 2). This assumes that the mathematical form of the model describes the true relationship.

Three parameters can be used in the basic IRT model. A one-parameter model involves the difficulty of the test item and the trait level (ability) of the test subject (Weiss, 1983: 9). If more than one parameter is needed to describe the test items, than a second parameter can be added. This parameter seeks to account for how quickly the probability of a correct response can change as a function of ability, or how well the test question can discriminate in ability level (Weiss, 1983: 9-10). Finally, a third parameter can be used to account for effects of random guesses (pseudoguessing), resulting in a three-parameter model (Weiss, 1983: 10). Equation 2-2 provides the Three-Parameter Standard IRT Model.

$$\Pr ob\{U \mid ability = \vartheta\} = \prod_{i=1}^{n} P_i(\vartheta)^{u_i}[1 - P_i(\vartheta)]^{1-u_i}$$

$$P_i(\vartheta) = c_i + (1 - c_i)\{1 + \exp[-a_i(\vartheta - b_i)]\}^{-1}$$

Equation 2-2 Three-Parameter Standard IRT Model

In this model, U represents a vector of scores on test items coded 1 for correct responses and 0 for incorrect responses, and $P_i(\theta)$ is the conditional probability that a randomly selected test subject with ability θ will correctly answer the *i*th question (Weiss, 1983: 112). The values of a, b, and c represent item discrimination parameters, item difficulty parameters, and aspects of pseudoguessing respectively (Weiss, 1983: 112). In the standard model, a test subject's ability is held to be constant during the test, responses are scored as correct or not correct, and θ is unidimensional (Weiss, 1983: 112).

Implementation of an IRT model requires estimation of values for the variables (observed and latent) (Weiss, 1983: 10). This progresses in two stages. First, the values of the parameters are estimated. This stage is often termed item calibration, and is carried out for each test item (Weiss, 1983: 10). Trait level parameters are obtained as a result of this effort, but are not the main focus at this stage (Weiss, 1983: 10). The second stage of implementation is estimation of the trait levels (ability) of test subjects using the item parameters from the previous stage (Weiss, 1983: 11-12). In this stage differences between individuals, in terms of ability or responses to test items, can be estimated (Weiss, 1983: 112). Different test subjects must be used for each stage (Weiss, 1983: 10).

Sample sizes, the number of items in the test, and other aspects of the data can affect the results (Weiss, 1983: 10). Aspects of the model's ability can be evaluated using tests for robustness and goodness of fit for a specific model (Weiss, 1983: 31). The more general IRT models, such as the three-parameter model, require more time to obtain parameter estimates, larger sample sizes, and more test items, but this model tends to provide a better fit of the data (Weiss, 1983: 31). Computer simulation is often used to explore these concepts, since data can be generated with known trait levels and item parameters (Weiss, 1983: 10, 33). In actual use, direct access to the test subjects is required to the extent that the subjects must take the test themselves.

2.8.4. Stochastic Token Theory

Stochastic token theory is based upon experimental psychology's traditional stimulus-response (S-R) paradigm. A subject is shown a precisely controlled stimulus, and he or she then responds using one of a specified set of reactions (Falmagne, 1997:129). Quantitative analysis of the data leads to inferences concerning what took place within the subject (Falmagne, 1997:129). Experimental psychology and related empirical social sciences theorize about what happens in the "black box" between the observed stimulus and response. Finite-state learning models assume that the subject can be in only one of a finite number of states at any time. The states are specified by their probabilistic ties to the stimulus and to the response (Falmagne, 1997:129). Parameters estimated from the data provide the connections. Learning is then the process whereby a subject moves from an initial state to a final state. While the stimulus and response are well characterized, little is known or postulated about the subject's states (Falmagne, 1997:129).

The stimulus-response paradigm has limited usefulness in cases where the stimuli are not under the control of the experimenter (Falmagne, 1997:129). An example is data for election polls if the polls use the same respondents over a period of time. If the respondents change their ranking of candidates between surveys, the experimenter does not know what exactly caused the change in preferences (Falmagne, 1997:129). In this case, the stimuli are unknown, but the responses (**R**) provide information about the respondents' state at the specific time intervals (t_i) (Falmagne, 1997:130).

This suggests use of a new model that uses the stimuli as the model's theoretical construct rather than the subject's state (Falmagne, 1997:130). A large data set results from all of the possible rankings of candidates over several time intervals (Falmagne, 1997:130). Statistical analysis of trends in the data can provide meaningful insight into the states and preferences of the survey population (Falmagne, 1997:130). The set of Stochastic Token Theory models is particularly suited to survey data, or other situations amenable to the same framework of unobserved states followed by observed responses over time (Falmagne, 1997:130).

The two fundamental constructs of Stochastic Token Theory are the states and the stochastic stream of tokens. At any time t, each member of the population is in one of a finite set of states in the class S (Falmagne, 1997:130). The states are fully or partly observable, for example the researcher could ask for a subjects most preferred political candidate at specific time intervals (Falmagne, 1997:130). If the preferences for all candidates are not specifically ranked, only features of the states are associated with the responses (Falmagne, 1997:130). S could also represent a set of semiorders (i.e. partial, interval, or weak orders) on the set of alternative A (Falmagne, 1997:130). The second construct, the stream of tokens, represent a collection of messages that bombard the subject. The information in each token could potentially move a subject from one state into another adjacent state (Falmagne, 1997:130). The model does not assume that the tokens can be reliably observed. Rather, their effect is seen through statistical analysis of the subjects' responses (Falmagne, 1997:130). In effect, the tokens map *S* back into *S* (Falmagne, 1997:130). The model specifically explores a collection of tokens *T* that generate a semigroup of transformations on *S* so that each token has a unique "reverse" (Falmagne, 1997:130).

A framework for stochastic token theory is that of subjects whose succession of states is the result of the random occurrence of tokens delivered by the environment (Falmagne, 1997:140). If tokens occur as if drawn with replacement from an urn, the result is a real time renewal process (Falmagne, 1997:140). A probabilistic token medium is specified by the quadruple (S, T, ξ, θ), where ξ is the probability distribution on the set of states and θ is the probability distribution for the set of tokens (Falmagne, 1997:140). The distribution ξ represents the beginning of the process, and θ governs the change of states due to the occurrence of tokens (Falmagne, 1997:140). These two distributions give rise to a discrete-parameter stochastic process -- a regular Markov chain on the set of states *S* (Falmagne, 1997:140). A regular Markov chain is homogeneous, irreducible, and aperiodic (nonrepeating) (Falmagne, 1997:140).

Several assumptions are required for the evolution of states in real time. Rather than assuming that tokens occur in discrete trials as if selected from an urn, assume that the tokens occur as a renewal process (Falmagne, 1997:141). If a token occurs at time *t*, then it is equal to τ with probability θ_τ (Falmagne, 1997:141). The times of occurrence of tokens is assumed to by a homogeneous Poisson process with intensity λ (Falmagne, 1997:141). The k-step transition probability of the Markov chain is completely defined by the probability of the tokens (Falmagne, 1997:141). The tokens are not assumed to be controllable or observable; only their accumulated effects can be observed or quantified by repeated probing the states over time (Falmagne, 1997:141-142). No assumptions are made about the internal structures of the states (Falmagne, 1997:142). This approach provides a general framework for exploring how preferences vary over time (Falmagne, 1997:143). The number of tokens is significantly less than the number of states, which is critical since one seeks to explain as many observable quantities as possible with a few number of theoretical constructs (parameters attached to tokens) (Falmagne, 1997:142).

2.8.5. Petri Nets

Petri Nets were developed to model systems, and are particularly useful with those having independent subsystems (Peterson, 1981: 31). The models are used to observe the occurrence of events and activities, to include the movement of information, in the system of interest (Peterson, 1981: 31). The Petri net developed can have multiple levels of detail, such as those commonly developed to represent computer hardware and software, or project plans (Pagnoni, 1990: 119; Peterson, 1981: 40).

Petri nets are built either to describe a proposed or existing system, or to analyze a system that can be described as a Petri net (Peterson, 1981: 151). Analysis efforts, which proceed in a similar fashion to analysis of networks, attempt to determine the properties of the Petri net and the system it represents (Peterson, 1981: 151). The set of all transitions (actions) that can occur characterize the system of interest, and is one of the most important properties of the system (Peterson, 1981: 151). Analysis techniques can explore the boundedness of the Petri net, the conservation of tokens in the system, reachability of places (events), set covering, and the matrix equations that correspond to the Petri net (Peterson, 1981: 91-112).

The two basic concepts used in Petri nets are events (transitions) and conditions (places) (Peterson, 1981: 32). The state of the system controls the occurrence of the events, and the system is described by its set of conditions (Peterson, 1981: 31). A given condition, which will either be evaluated as "true" or "false", represents a logical description of the state of the system (Peterson, 1981: 31).

The preconditions of an event are those conditions that must hold true in order for the event to occur (Peterson, 1981: 31). Additionally, an event can result in new conditions (postconditions) becoming true and / or in some preconditions becoming false (Peterson, 1981: 31-32).

In modeling terms, the preconditions represent the inputs of a transition (event) and the postconditions represent the outputs (Peterson, 1981: 32). Tokens are used to represent the conditions in the system. A token is located at every place (condition) that holds true. When a transition (event) occurs, the tokens are removed and new ones are placed for the postconditions (Peterson, 1981: 32-33). Multiple events that are enabled can occur simultaneously if they are independent (Peterson, 1981: 35).

Time need not be explicitly modeled, as the Petri net structure contains all of the information needed to define the possible sequences of events (Peterson, 1981: 36). When multiple transitions are enabled, the choice of which one fires first is made randomly (Peterson, 1981: 36). The events are assumed to be instantaneous, and events cannot occur simultaneously (Peterson, 1981: 37).

Events that are not instantaneous in the system of interest can be modeled using two events, one for the start time and another for the end time, and a condition for the event occurrence (Peterson, 1981: 37-38). If the net is executed multiple times, the duration and sequence of events will differ (Pagnoni, 1990: 120).

Events that lay on the same path through the network are causally dependent (Pagnoni, 1990: 119). This dependence can be a function of time, resources, or other precedence constraints (Pagnoni, 1990: 119). Equivalently, those events that do not lie on a common path are seen as causally independent (Pagnoni, 1990: 119).

A Petri net's structure, C, is represented by four elements: a set of places (P), a set of transitions (T), an input function (I), and an output function (O) (Peterson, 1981: 7). The set of places and transitions are finite and disjoint (they do not overlap) (Peterson, 1981: 8). Additionally, the input function maps from the set of transitions to the set of places, and the output function does the reverse (Peterson, 1981: 8).

The final element of a Petri net is the set of tokens, discussed previously, that are used to mark the execution of the net (Peterson, 1981: 8). The number of tokens and their positions may change during execution, as they represent the occurrence of transitions (Peterson, 1981: 8). The number of possible tokens in a given place on the net is infinite; therefore there are infinite ways that the tokens may form a "marking" of the net (Peterson, 1981: 17). A marking is an assignment of tokens to places in the net based upon the conditions of the system (Peterson, 1981: 16). The set of all markings is then countably infinite (Peterson, 1981: 17).

2.8.6. Random Utility Models (RUM)

Another approach to modeling hackers is from the perspective of Thurstonian Models, a subset of Random Utility Models, also known as Stochastic Utility Models. Stochastic utility models seek to account for situations where preferences are probabilistic or random, hence the use of the term stochastic (Barbera, Hammond, and Siedl, 1998: 275). They are suitable when different choices are to be made in similar situations, and therefore could help explain why people may make different choices for the "same" decision at different times, or why individual members of a group have different preferences for alternatives when presented with the same decision. Thurstonian models explore how to extrapolate from data how the group, as a whole, thinks. It is therefore a descriptive class of models.

Thurstonian models utilize three basic assumptions: continuous preference between pairs of stimuli, the stimulus that is preferred by the subject at the time of solicitation has a higher value, and populations have preferences that are normally distributed (Maydeu-Olivares, 2000: 3). This basic preference model can be used to fit rankings or, by use of a threshold relationship between unobserved preferences and observed responses, a extended model could be used to fit rating data (Maydeu-Olivares, 2000: 3). Interestingly, it is not assumed that the stimuli are judged independently. However, these models are not used in many applications since they often require a many dimensional multivariate normal integral be calculated to obtain the ranking, paired comparison, or rating preference probabilities (Maydeu-Olivares, 2000: 3). This results from the large number of comparisons that must be made for every stimulus.

Some attempts have been made to estimate and test Thurstonian models with only limited information. The model uses just the first and second order marginal probabilities from contingency tables (Maydeu-Olivares, 2000: 3). This approach has been used several times in psychological experiments, and is now being extended to rating, ranking, binary, and graded paired comparison data (Maydeu-Olivares, 2000: 4).

A three-step procedure is used to estimate and test the model, along with a goodness-of-fit test developed by Maydeu-Olivares (Maydeu-Olivares, 2000:4). The procedure uses grouped data to restrict the thresholds and underlying correlations in the normal random variates. This procedure works well for polytomous data (data with many categories). Ungrouped data are used when additional data on the subject or stimuli are to be modeled along with the preference data (Maydeu-Olivares, 2000:4).

Paired Comparison Thurstonian model

When complete paired comparison experiments are conducted, a random sample of N individuals from a population are asked to compare all pairs obtained from a set of n stimuli. This results in ñ = n(n-1)/2 pairs of comparisons, where the subject is asked to select a preferred option in each pair. The outcome in each case is represented as a random variable y_i, where $y_i = 1$ if the first option is preferred, and 0 otherwise. This results in a Bernoulli random variable, with the overall joint distribution for all n y_i is that of a multivariate Bernoulli distribution (Maydeu-Olivares, 2000:5).

Modeling seeks to explain the observed preference patterns of paired comparison from an n-dimensional vector of unobserved continuous preferences **t** and a ñ-dimensional vector of random errors **e** associated with each paired comparison. The preferences are assumed to be approximately normal (μ_t, Σ_t), and errors are assumed approximately normal (0, 0 Ω), where Ω is a diagonal matrix. The model becomes

$$y^* = A^*t + \varepsilon$$

Equation 2-3 Thurstonian Paired Comparison Model

A is a ñ x n matrix of contrasts where columns are individual stimuli, and rows are the paired comparisons (Maydeu-Olivares, 2000:6). The variables **y** can be obtained from the unobserved **y***, and the usual standardization of **y*** results in a standard normal **z*** with mean zero. The covariance matrix for **z*** has diagonals of 1, Ω is assumed to be I, and $\sigma_{ii} = 1$ for all *i* in n (Maydeu-Olivares, 2000:7). Finally, $\mu_t = 0$ is chosen arbitrarily due to location indeterminacy in the elements of Σ_t (Maydeu-Olivares, 2000:7).

Ranking Thurstonian Model

In the case of a ranking experiment, the subjects rank all of the stimuli according to a specified preference criteria function. This would result in n! possible permutations of the rankings, giving a multinomial sampling distribution. This can be transformed to a ñ -dimensional multivariate Bernoulli by defining y_i as a dichotomous variable of ordered pairs of stimuli. A given y_i is assigned a value of 1 if y_i is ranked above y_j, and 0 otherwise. The multivariate Bernoulli distribution's contingency table must be filled with an additional $2^{\tilde{n}}$*n zeros since only n! ranking patterns are possible (Maydeu-Olivares, 2000:6).

The parameters of the ranking model are based on the ordered pairs of comparison data. The population's unobserved continuous preferences have mean μ_i and variance σ_{ii}, and the correlations between preferences for any two given stimuli are ρ_{ij}. The final parameter, ω_{ij}, is the variance of the random errors e_{ij} associated with each paired comparison (Maydeu-Olivares, 2000:8). The random errors in **e** allow modeling of intransitive patterns in the paired comparisons, which Maydeu-Olivares deems crucial. Intransitive patterns of preferences allow subject's preferences to change during the experiment as a stimulus is presented next to several different stimuli. As a result, the random errors are assumed to be uncorrelated with both the continuous preferences **t** and each other. The covariance matrix is then diagonal (Maydeu-Olivares, 2000:8).

Rating Thurstonian Models

In a complete rating experiment, each stimulus is presented alone, and a preference is assigned according to a binary rating scale. The outcomes can then be represented by y_i as above, and the resultant joint distribution is again multivariate Bernoulli (Maydeu-Olivares, 2000:5).

With the unobserved continuous preferences **t** defined as for paired comparisons, a threshold α for the preference is assumed to exist. Therefore, the binary variables **y** are assumed to be $y_{ij} = 1$ only if $t_{ij} \geq \alpha$, and 0 otherwise (Maydeu-Olivares, 2000:9). The probability patterns are unchanged for the transformation to **y***. The result is

$$\begin{gathered} y^*_i = \alpha \\ \sigma = 1 \end{gathered}$$

Equation 2-4 Thurstonian Rating Model

for all *i* and μ_n is assigned a value of zero (Maydeu-Olivares, 2000: 9).

Application to Survey Data

Thurstonian models have also been used to model purchases of consumer goods. Some of the models attempt to gain insight into aspects of consumer choice otherwise masked by use of only aggregated choice data (Islam, Louviere, and Bartels, 2000: 2). One approach by Islam, Louviere, and Bartels uses depth of repeat given trial, or purchase incidence given trial, as count data for the model. Individual repeat choices are modeled as Poisson a process, with purchase rates in the population as a whole having a gamma distribution. This results in a negative binomial (NBD) model (Islam *et. al*, 2000: 2). The resulting Markov chain style model has stationary purchase rates and the usual memoryless property for purchase times.

A second approach models the inter-purchase times. The goal is to better understand and model the dynamics of purchase behavior (Islam *et. al*, 2000: 2). Inter-purchase times are assumed to be exponential random variables, leading to a Pareto distribution (Islam *et. al*, 2000: 2). This model can be extended by the use of flexible parametric baseline hazard models, non-parametric proportional hazard rate models, and modeling heterogeneity using multivariate normal distributions (Islam *et. al*, 2000: 2).

Both of these approaches use discrete trials, which is adequate when a single unit of the consumer good is purchased in each trial period. If multiples are purchased, another approach is to model purchase amounts conditional on choice behavior (Islam *et. al*, 2000: 2-3). The result is a Beta-Binomial model framework.

Comparisons between the modeling approach can be made through the use of the following two questions (Islam *et. al*, 2000: 3-4):

1) Do differences exist between consumers who do not try a product and those who try but do not repeat, those who try once and repeat once, etc?
2) Can a consumer choice model be developed to purchase volumes conditional on amount of repeat purchases?

To explore these questions, Islam, Louviere, and Bartels hypothesize that there are systematic differences in the personal characteristics of consumers who never try a product, those who try but never purchase the product again, and those who repeat purchases a given number of times (Islam *et. al*, 2000: 3). If the purchase behaviors are given the role of states, then personal characteristics such as age and number of household members, and the period of life they are in, would represent stages (Islam *et. al*, 2000: 3). The question can then be explored using a random utility model in which the latent (unknown) preferences of the households would predispose them to one of the states. The assumption is made that the random aspects of the utility are IID (independently and identically distributed) extreme value type I random variates, which results in a discrete discriminant model (unconditional logistic regression) (Islam *et. al*, 2000: 3-4). Additionally, the authors develop a method of modeling purchase volumes given number of repeat purchases (Islam *et. al*, 2000:4).

The behavior choices of the consumers are treated as a series of inter-related choices (Islam *et. al*, 2000: 4). This approach allows the model to develop in the context of a random utility model. Consumers choose outcomes that they most prefer, or that maximizes their utility, subject to any constraints (Islam *et. al*, 2000: 4). The consumer's true utility cannot be measured, resulting in a latent utility model (Islam *et. al*, 2000: 4).

$$U_{in} = V_{in} + \varepsilon$$

Equation 2-5 Consumer Preference Model

U_{in} is the utility (true or latent) of choice *i* for consumer n. V_{in} is the systematic model component that is observable or experimentally estimable, and ε_{in} reflects the fact that not all factors influencing consumer *n*'s choice can be directly known (Islam *et. al*, 2000: 4). In this framework, it is easy to understand the inherent stochastic nature of the situation, since one cannot exactly predict a consumer's choice, but one can estimate the probability that a consumer will make each of the available choices (Islam *et. al*, 2000: 4).

2.9. Total Quality Management (TQM) and Fishbone Diagrams

The model that was finally selected was the Ishikawa "fishbone" diagram. Details of this method are presented in Section 3.1. The strengths of this method include its clear and elegant visual nature. Unlike models such as VFT, the result is not a "number" for a given alternative being considered.

Placing a numerical value on an individual's profile can be misleading. What does the number mean? What does it mean that one group's average member scores a value of *x*, while another group's scores a value of *y*? Is there a true significance in the difference between the two numbers, and what is the true precision of the number reported? In the case of a profile for an individual that has not been extensively interviewed, a numerical value produced by a model may mislead decision makers as to the capabilities and granularity of the tool being used.

What is desired from the model being developed is a description of the person. This is provided by the Ishikawa diagram. Both VFT and Ishikawa diagrams make use of group expertise in building the model. This is vital with profiling, since input from various types of experts is required. Ishikawa diagrams also allow for factors that are interrelated. Human nature is hard to separate into a few, mutually exclusive, areas. Models such as VFT require that the categories used by both mutually exclusive and collectively exhaustive.

Table 2-6 highlights the strengths and weaknesses of the models explored in this section.

Table 2-6 Summary of Models Explored

Model	Strengths	Weaknesses
Value Focused Thinking (VFT)	• Group process • Additive model • Numerical result • Level of detail • Sensitivity Analysis	• Group process • Weights depend upon level of decision maker •Score every aspect •Measures mutually exclusive, collectively exhaustive
Item Response Theory (IRT) / Latent Trait Theory	• Psychology model •Numerical result •Indicative of underlying preferences	• Single factor analyzed • Experimental nature • Validity for small data sets, and level of abstraction • Requires direct contact with hackers
Token Theory	• Level of detail • Flexible	• Cause & Effect relationships • "Project" style path • Order of choices • Requires direct contact with hackers
Petri Nets	• Level of detail • Flexible	• Cause & Effect relationships • "Project" style path • Order of choices
Random Utility Model (RUM)	• Similar to VFT • Preferences under uncertainty • Additive model • Numerical result • Level of detail • Sensitivity Analysis	• Weights depend upon level of decision maker • Score every aspect • Measures mutually exclusive, collectively exhaustive • Requires direct contact with hackers
Ishikawa Diagram	• Group Process • Qualitative & Quantitative data • Visual nature • Analysis through Pareto charts, control charts, etc.	• Group Process • No single numerical result

2.10. Summary

The topics and documents discussed provide a basis to begin analyzing malicious hackers. Chapter Two was developed to consolidate information on the major areas that have bearing on building a malicious hacker profile. References on hackers and criminal profiling and US military doctrine were summarized separately (rather than integrated) so that the authors' ideas could be presented as a cohesive whole. The following chapter will use the knowledge gained from the sections of Chapter Two to develop a model framework applicable to analyzing foreign IO programs that utilize malicious hackers.

3. Malicious Hacker Framework

3.1. Introduction and Methodology

A profile of any individual is complex. Many aspects such as personality, motivation, education, and group membership affect what makes a person who they are. This makes it difficult to develop a clear, concise model that is easy to present, understand, and execute.

The model found to best represent a scripted profile of structured hackers, given the current level of available open source data, is the Ishikawa "fishbone" diagram (cause-and-effect diagram). A fishbone diagram visually presents the main profile areas, and allows for additional levels of detail to be developed as required. It is also one of the most widely used quality control tools (Costin, 1994: 177). One key advantage of this approach is the ability to examine each profile area in turn, keeping only the details from a "basic malicious hacker" model that applies to the specific group or individual being investigated. Results from each of these areas are then combined to form the overall profile. A description of the fishbone diagram process is presented below, followed by the development of the basic model.

3.1.1. Fishbone (Cause-and-Effect) Diagrams

Fishbone diagrams were developed as a method for identifying and clarifying the underlying causes of a problem. As a quality improvement tool, they are often used for solving problems within industrial processes. Their use can complement control charts in deciding what changes to make when a process has gone out of control (Mitra, 1993: 6). Fishbone diagrams are sometimes called "Ishikawa diagrams" in honor of the quality expert, Kaoru Ishikawa, who championed their adoption for problem solving in 1943 (Mitra, 1993: 6; Ozeki and Asaka, 1990:149). They resemble "fishbones" in that suspected causes or factors relating to a problem surround a core "spine", which connects to an effects side representing the problem at hand (Mitra, 1993: 6). Figure 3-1 presents an example fishbone diagram. The "causes" are believed to influence the "effect", and the goal of the process is to find out in what way the influences exist and to resolve them. The common areas of causes that are explored are materials, machinery and equipment, operating methods, manpower (operators), policies and procedures, measurements, and environmental factors (Winchell, 1991: 89).

Two types of cause-and effect diagrams exist – "how" and "why" diagrams. The "how" chart focuses on how a problem can be solved (countermeasures) rather than explaining the causes of the problem. "How" diagrams run the risk of focusing on symptoms of the underlying problem(s) rather than the root of the problem. "Why" diagrams instead focus on why the problem arose (underlying causes). As a result, any solutions developed should deal directly with the root cause of the problem rather than just the symptoms (Ozeki and Asaka, 1990: 36-37).

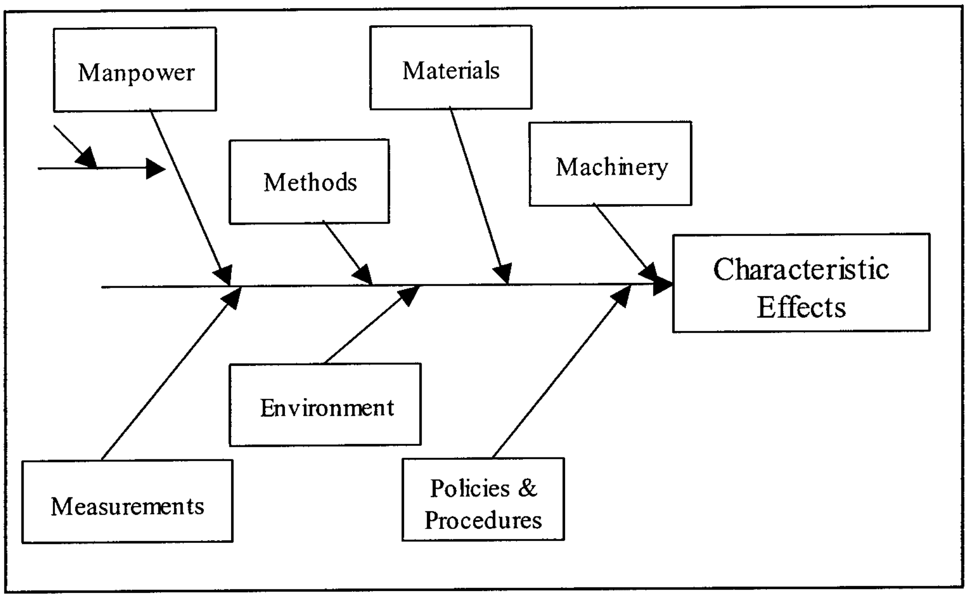


Figure 3-1 Example Fishbone Diagram

Ozeki and Asaka point out that fishbone diagrams serve many purposes (Ozeki and Asaka, 1990: 157). They can help guide discussion about a problem by providing a process on which to focus. The diagrams may provide insights that might otherwise have been missed, and may aid understanding and process observation. Key interrelationships among aspects of the problem may become more evident (Mitra, 1993: 142). Unlike Value Focused Thinking, the Ishikawa diagram's factors need not be mutually exclusive. With its focus on the "big picture", broader environmental areas are addressed that might otherwise be ignored as not "controllable" (Costin, 1994: 182).

Additionally, these diagrams can be used to gather frequency data for problem causes during day-to-day operations. In the case of a malicious hacker profile, this might consist of frequency counts for characteristics as data becomes available to "feed" that aspect of a specific group or individual's profile. A Pareto chart would provide a useful tool to track those details of an aspect occurring most frequently (Mitra, 1993: 191). Pareto charts can be used to identify areas that are causing the most problems, so that resources used to remedy those problems will provide the most improvement while utilizing limited resources in the most efficient method possible (Mitra, 1993: 140). The chart consists of the data categories along the horizontal axis and the percent of cumulative occurrence on the vertical axis. Data categories are presented in decreasing percentage of occurrence (Mitra, 1993: 140). Figure 3-2 provides an example Pareto chart. The left vertical axis provides the percentage of occurrence for each of the four problem types, and the right vertical axis provides the cumulative percentage. As an IO example, incidents that support an IO organization's use of a specific hacking process or tool would provide a count, helping to focus Information Assurance efforts on appropriate defensive measures. Changes in tool usage or hacking approaches could be tracked over time to maintain an updated assessment of adversary intents and potential actions.

The combination of cause-and-effect diagram and Pareto analysis ensures effort is extended only on those factors that provide the "most bang for the buck", rather than tangential issues (Mitra, 1993: 584). The Pareto chart often upholds the 80-20 rule – 80% of a problem is caused by 20% of the factors involved (Winchell, 1991: 86). Inventory control theory also provides the ABC policy (90% of the cost belongs to 10% of the parts) is a similar concept (Nahmias, 1993: 272-273).

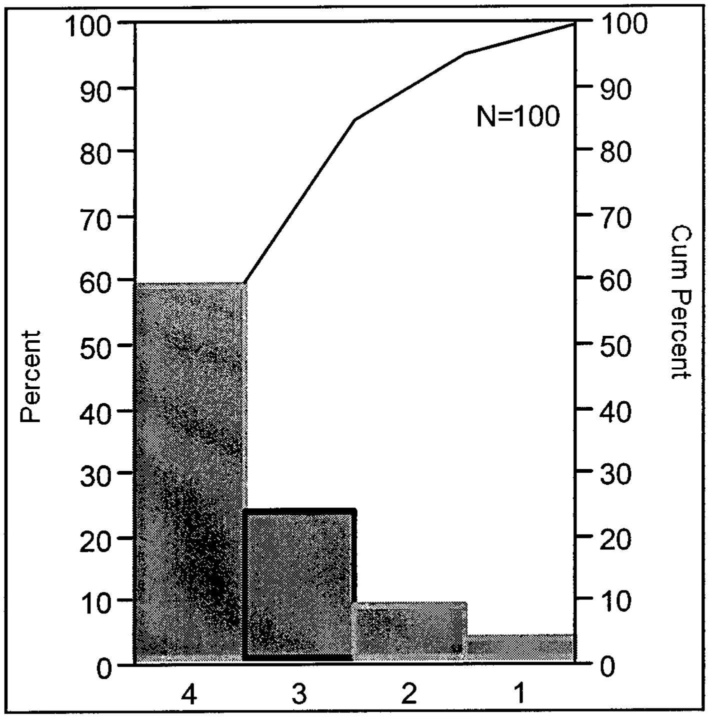


Figure 3-2 Sample Pareto Chart

Finally, Ishikawa diagrams can be used with a stable process to identify areas for further improvements (Mitra, 1993: 142). The malicious hacker framework developed can be used to identify areas for expanded profiles in the future. More useful model details could replace those that cannot be substantiated, and additional levels of detail can be grown as required. Additionally, the malicious hacker model developed would provide a basis for profiling other groups of hackers, such as script kiddies or those hackers who are not members of structured groups.

The process of creating a fishbone diagram is easy to learn and implement (Costin, 1994: 177). Developing a cause-and-effects diagram involves six steps, summarized in Table 3-1. An individual can implement the process; however, it is best used when the input of a team is available (Costin, 1994: 177). The team involved should be broad-based, but of a small enough size that the brainstorming process remains productive (Costin, 1994: 183). In Step 2 and 4, care should be taken not to unduly eliminate potential factors early in the process (Mitra, 1993: 143). Without further analysis, one of the root causes of the problem may be ignored. Lower level causes can be repeated under higher-level categories if direct, multiple relationships exist (Costin, 1994: 179).

Three methods exist for adding levels of detail to the fishbone's spine (Step 3): big branch expansion; brainstorming; affinity diagrams. Big branch expansion begins by identifying a few key causal areas. As mentioned earlier, in production situations, these often consist of materials, machinery and equipment, operating methods, manpower (operators), and environmental factors (Ozeki and Asaka, 1990: 150). A main branch is drawn from the causal area (placed within a box frame) to the spine. Additional branches pointing to the main factor provide increasing levels of detail (Ozeki and Asaka, 1990: 151).

Table 3-1 Ishikawa "Fishbone" Diagram Process

Step	Details
1: Clarify characteristics	Choose a title for the problem. Ensure everyone understands the problem. Determine characteristics to examine.
2: Draw spine and effects characteristics	Describe the effect characteristics to be explored in specific terms. Draw the "spine" or "trunk" for the diagram as an arrow pointing to the effect characteristics.
3: Clarify factors affecting the characteristics	Identify and define the factors that could cause the effect characteristics. Methods: big branch expansion; brainstorming; affinity diagrams.
4: Check for omitted factors	Ensure no factor has been left out. The diagram may need updating over time.
5: Identify factors that strongly affect the characteristics	This step helps identify the most critical factors; those that provide the most explanation of the characteristics observed.
6: Adding related information	Add clarifying information, as well as date of creation and names of participants.
	Source (Ozeki and Asaka, 1990: 150-157).

Brainstorming, also called small branch expansion, begins with a group brainstorming exercise to identify all factors that might affect the problem at hand. These factors are then grouped into small functional categories. Smaller categories provide the lowest level of detail that is then grown into higher levels, ultimately connecting to the fishbone's spine (Ozeki and Asaka, 1990: 152). The third method, the affinity diagram, is also referred to as small branch expansion (Ozeki and Asaka, 1990: 153-154). The only difference is that the affinity diagram process is used as an alternate form of brainstorming. Instead of a group brainstorming session, each participant brainstorms separately. Pieces of paper are divided among the group. Participants record a single potential cause on each piece of paper. All of the cards are then placed on a wall or table, and the group as a whole decides on a category framework as in the brainstorming process.

The greatest benefit of the cause-and-effect diagram comes from turning the analysis into action. The aspects of the problem should be quantified where possible (Costin, 1994: 182). Pareto charts, mentioned earlier, are one possibility. Care must be taken, however, in selection of parameters to measure. Their relationship to the factor of interest must be clearly established, and the parameter must be well defined.

3.1.2. Basic Hacker Framework Approach

Profiles of hackers can be made at various levels of detail, as shown in Figure 3-3. The goal of this effort is a profile of malicious hackers that belong to a state-sponsored, or other structured, group. This represents Step One of the Ishikawa diagram process. The title for the problem is "Malicious Hacker Profile".

An Ishikawa diagram framework will now be developed that addresses the key factors seen to influence hacker behavior for the group being studied (Step Two). Those factors are *Motivations* and *Personality*; *Approach* to hacking; individual *Skill* and aspects of *Teamwork*; hacker *Tools* and *Training*; the *Intent* of actions, their *Timing* and *Use*; *Cultural Impacts*; and, *Leadership, Doctrine* and *Policy.* A parallel can be seen with the traditional factor categories of operating manpower (operators), methods, materials, machinery and equipment, measurements, environmental factors, and policies and procedures. Figure 3-4 presents the basic framework.

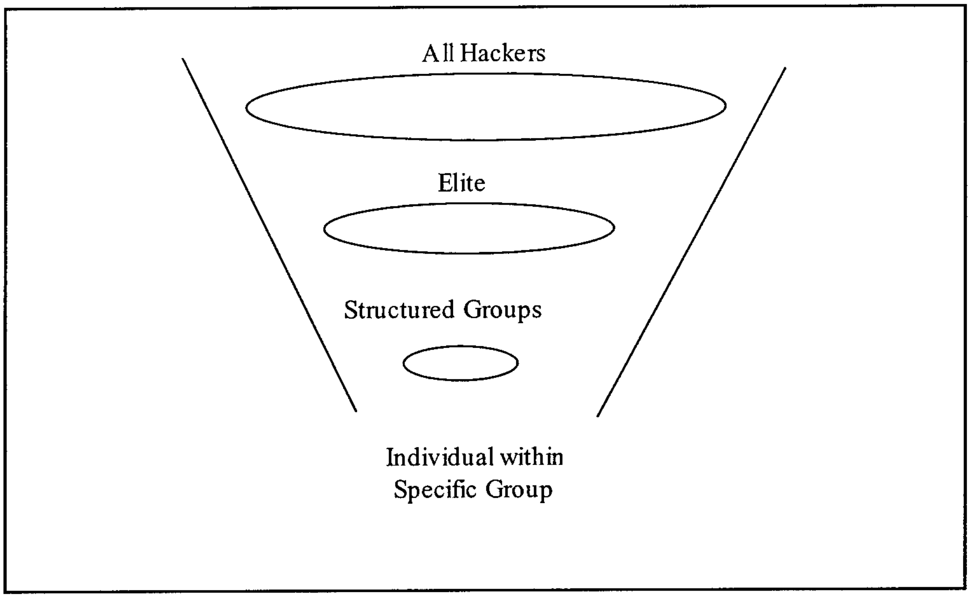


Figure 3-3 Hierarchy of Hacker Profiles

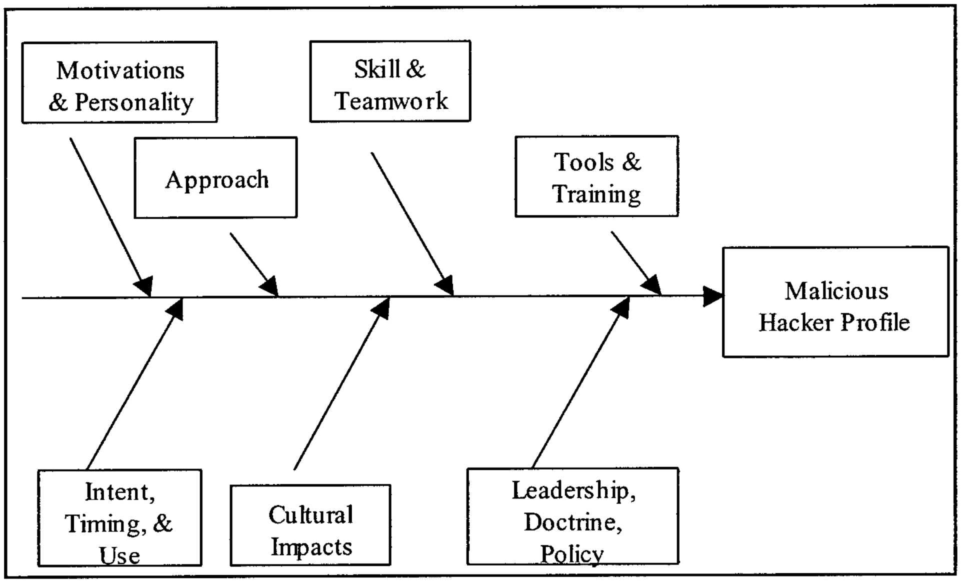


Figure 3-4 Basic Framework

Following each factor is a diagram representing the details for that factor.

3.2. Motivations and Personality

What makes someone hack? What makes them hack at the behest of their country, their terrorist organization, or the transnational criminal organization to which they belong? Are common personality characterists shared among hackers? While profiling in general seeks to find unique aspects of the individual or group profiled, in some instances a common personality characteristic may provide the best chance for influencing a hacker once he has been identified.

3.2.1. Hacker Motivation in General

Many authors on hackers discuss a range of motivations for hacking. These motivations can apply together in groups or individually for each hacker. Some motivations may change over time. Taylor discussed boredom with school as a motivation for hacking (Taylor, 1999; 52). When a hacker moves on to college, this motivation might diminish. While the authors in Chapter 2 discussed many motivations, this model will only utilize those most likely to correspond to the motivations of the target groups. Several of the other motivations discussed in Chapter 2 would have a direct bearing on terrorist groups and criminals. Those motivations that are felt to have the most bearing on nation state hackers are summarized in the following table.

Table 3-2 Malicious Hacker Motivations

Motivation	**Definition**	**Sources**
Curiosity	The desire to learn and explore.	(Chantler, 1996: 108; Denning, 1999: 45; Taylor, 1999: 46)
Challenge	The desire to achieve, as well as the thrill of an illicit pursuit	(Chantler, 1996: 108, 126; Denning, 1999: 45)
Recognition	Hacking can provide social benefits such as a close circle of friends, and peer recognition. This can also relate to aspects of patriotism, nation prestige, and unit or Service pride.	(Denning, 1999: 45; Taylor, 1999: 58 - 60; Vranesevich, 2000)
Personal Satisfaction	A sense of accomplishment. Pride in self.	(Chantler, 1996: 108; Denning, 1999: 45)
Feelings of Power	The desire to have control over a system, or to feel "better" than the system administrators.	(Denning, 1999: 46; Taylor, 1999: 56; Vranesevich, 2000)
Governmental	Acts directed by one government against another (IW and espionage) in support of national objectives.	(Vranesevich, 2000)

3.2.2. Personality

Several common personality characteristics emerge as being common to hackers. Again, this may make them less useful in profiling hackers, but may provide important leverage points to influence them. First, by the nature of the task, elite hackers tend to be very detail oriented. This can be seen in the process they use to gather information on a target (McClure, *et. al* 1999: xxvi; Chantler, 1996: 109). According to Chantler, elite hackers may occasionally "short-circuit" this process in the hopes that success is possible without all of the information originally deemed necessary, less skilled hackers tend to be less thorough (Chantler, 1996: 109). Taylor likens this to just "rattling the doors" in the hopes of success, rather than planning for success (Taylor, 1999: 102).

A second characteristic of many hackers is their persistence. They spend a large amount of time and effort in order to exploit a target system. Information about the system, the information it holds, its vulnerabilities, and even what other systems it is connected to, is built over time. Only low-level hackers, or ones who wish to appear as such, just bash at a system in the hopes of success. Denning comments on one highly successful hacker Phantom Dialer, whose exploits were not attributable so much to "brilliance or skill …, but to an incredible persistence" (Denning, 1999: 46). This is what makes DoS and DDoS attacks interesting. While they are often seen as the last ditch effort of a frustrated script kiddie, many authors see them as the weapon of choice for terrorists and nation states seeking to deny access to a system (AFDD 1, 1997: 24; Lesser, *et. al*, 1999: 41; McClure, *et. al*, 1999: 340-341).

A third personality aspect is self-esteem. Chantler explored self-esteem as part of his survey of hackers. Interestingly, the level of self-esteem corresponded to skill level. Elite hackers were judged to have high self-esteem. Those of moderate skill were seen as having average or moderate self-esteem. These two groups are those that Chantler also believes to have "positive" motivations for hacking (Chantler, 1996: 126). Those with low self-esteem were also seen as having "negative" motivations (profit, vengeance, desire to cause damage) for hacking, and possessed of little skill.

Next, one can consider aspects of creativity. Elite hackers are seen as very creative (Chantler, 1996: 23). This, along with persistence, can be seen as a key to success. An elite hacker does not see obstacles in the same way that a system designer or administrator does; the hacker assumes there is a way around every obstacle and is very creative in seeking solutions.

A final aspect of personality that can be explored is the degree to which someone is a self-starter or a follower. This again can affect how the hacker is influenced. A follower may cease action when the leader is removed in some manner, whereas a self-starter will continue as long as they desire to do so. Additionally, influencing the leader succeeds in influencing all of his or her followers. Members within a group may be self-starters or leaders. In most cases, the leaders will be self-starters, as they "set the pace" for the group and develop new tools and techniques. Chantler sees the elite group of hackers as being the self-starter types; those with moderate skills are seen as followers (Chantler, 1996: 126). Followers reuse past exploits as they develop their own skills.

3.2.3. Mercenaries

Military members are seen as primarily motivated by patriotism, especially in all-volunteer forces such as that of the United States. Monetary payment is a secondary concern. Mercenaries, or hired experts, are primarily motivated by money, and may only feel a secondary tie to the country that has hired them (Machiavelli, 1962: 72). Close ties are to the mercenary group to which they belong, highlighting the need for a strong sense of trust in their own leadership.

With less of a tie to the success of the country for which they are fighting, mercenaries are generally seen as focused on personal survival ("live to fight another day"). If the danger of an operation gets too high, as discussed in Section 2.6, they may demand more money or leave the engagement. While hackers may be seen as placed at less risk of physical danger, this may not always be the case. Vranesevich discusses one method of preventing hacks – letting the hacker know you know their "true" identity (Vranesevich, 2000). This means that their anonymity has been compromised, and makes it easier for law enforcement to pursue them. While this may not be as effective against a military member, it may threaten a mercenary's future employment.

Other cases where a mercenary might feel threatened are: situations where the mercenary is co-located with military forces, or where the IW cell is co-located and can then be attacked. When mercenaries (or government groups) utilize the flexibility of communications and computing technology to transcend issues of location, it is significantly harder to hold their personal safety at risk.

3.2.4. Issues of Criminality

Hackers "know" what they are doing is "wrong" (a cultural element), but in the case of government hackers, their actions are sanctioned by the organization. This is similar to the case of assassins. As discussed in Section 2.2, international law is expanding to accommodate the growth of IW.

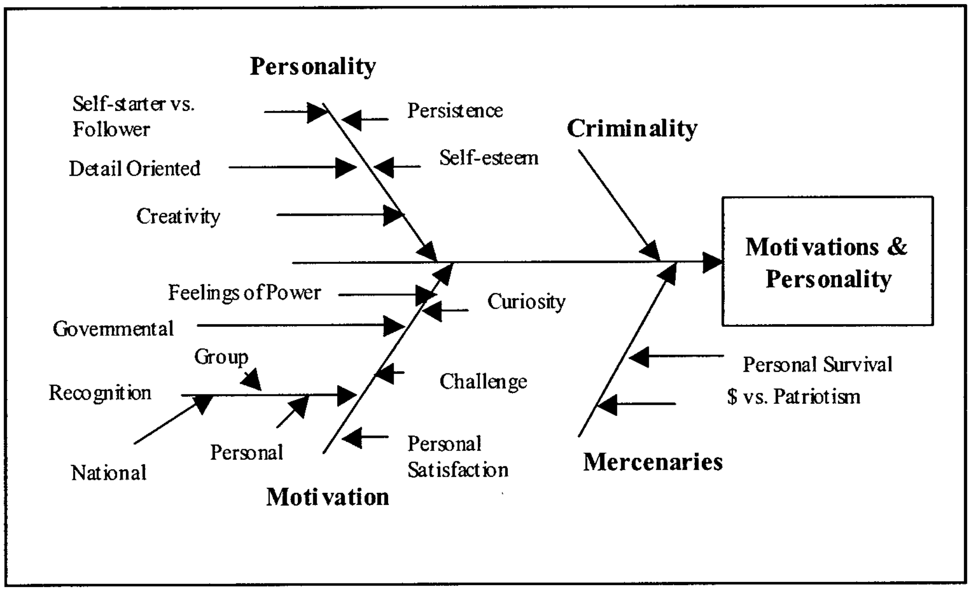


Figure 3-5 Motivations and Personality

3.3. Approach to Hacking

There are two basic approaches to hacking – unstructured and structured. Script kiddies and others of lower skill level are primarily the hackers utilizing unstructured approaches. Taylor refers to this approach as "rattling the doors" (Taylor, 1999: 102). McClure, *et. al*, talks of script kiddies that "throw everything they have" at a system rather than use a more formal process such as vulnerability mapping (McClure, *et. al*, 1999: 34). A more skilled hacker might utilize what appears to be an unstructured attack in order to blend in with script kiddies and avoid detection.

Structured attacks utilize a formal methodology, and might be referred to as "doctrinal" in nature (Lemon, 2000). Nation states' with developed IO organizations could be more likely to act under a structured methodology, especially once expertise in the field of IO has been trained or bought. In this light, the term "structured" can take on two meanings – an organized method of problem solving, and a method of conducting operations in accordance with formal military doctrine. The first meaning will be addressed in this factor, and the latter is considered in the *Leadership, Doctrine* and *Policy* factor. McClure *et. al* lists five steps in a basic attack (problem solving) methodology: target acquisition and information gathering; initial access; privilege escalation; covering of tracks; and planting of back doors (McClure, 1999:xxvi). These steps are discussed in Section 2.3.2. Detection of this process would require that events of the various attacks be noticed, associated in to a group, and analyzed as a common incident.

Chantler provides a methodology that he feels represents information processing by hackers with moderate to expert skill levels. This view is based upon his experience as head of computer security for the Australian Army, as well as many years of interviews with hackers and the ethnographic study performed for his doctoral dissertation. His work is reviewed in Section 2.3.3. Chantler compares the hackers' information processing to that of a military intelligence process (Chantler, 1996: 109). The process has three steps: direction, collection and collation, and dissemination. In the direction stage a target system or problem to solve is selected. Information needed to complete the task(s) is determined. The second step has two phases. First, the necessary information is collected, and possibly stored. Other members of a group may be asked to provide assistance. Next, the information is collated and analyzed. The third stage consists of either dissemination of information if the hack is successful, or beginning the cycle again if the hack is not successful (Chantler, 1996: 109). An interesting situation sometimes occurs in which a hacker breaks the cycle to test for success early (Chantler, 1996: 167). The goal is to complete the hack more quickly.

Discussions with Red Teams, or other members of United States IO organizations may provide valuable insight into structured approaches to hacking. These groups might, however, be loath to openly disclose their methods or tools. Interestingly, NSA director Lt. General Michael Hayden has openly stated that the NSA remains behind much of the world in "keeping up" with information technology developments (Verton, 2001).

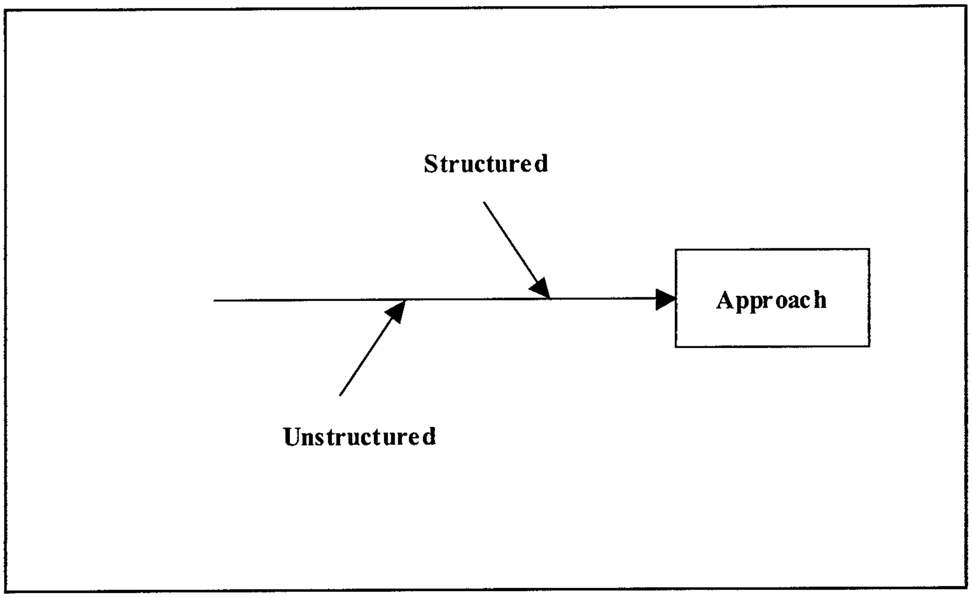


Figure 3-6 Approach

3.4. Individual Skill and Aspects of Teamwork

While hackers in IO organizations may most likely work as part of a team, their individual skill level remains an issue. Much of the open literature on hackers refers to hacker skill levels in various general categories. Psychological models such as Item Response Theory (reference Section 2.8.3) could provide a capability-based differentiation among skill levels of hackers. This would, however, require an adequately sized sample of hackers at all possible skills levels that were willing to have their skills tested, and that actually performed on the test to their best ability. Therefore, models of hacker skill levels will continue to revolve around self-reports and surveys, interviews with experts, and expert judgment for the near future.

In the case of both individual skill and teamwork, the various events involved must be tied together into common incidents. There is also the issue of tying events by the same individual or group together over time, even while their skill levels, team membership, motives, and methods are changing. This is a similar set of problems to those identified by Godwin for serial killers, as discussed in Section 2.4.1.

3.4.1. Individual Skill Levels and Talent

Chantler describes three skill or knowledge levels in his hacker profile. These consist of low, medium, and high levels. When developing a profile of members of a nation's IO organization, both individual skill and that of the "average" group member can be considered.

Those on the low category consist of hackers who display little evidence of intellectual capability (Chantler, 1996: 126). This group is termed "Losers" or "Lamers" by other hackers, and could be used to describe script kiddies. They may be using tools and techniques without understanding how or why they work (Taylor, 1999: 88). In Chantler's hacker survey, 193 respondents described the skill level or profile of hackers as expert / specialist, malicious, and nebulous. Both low and medium levels of hackers, as characterized by Chantler, belong to the nebulous category (Chantler, 1996: 113). Hackers with low skill levels may have just begun hacking, or are just disregarded by higher-level hackers. Their ability may be hindered by lack of education (Chantler, 1996: 126).

Both McClure and Lesser believe that Denial of Service (DoS) attacks will be used more extensively in the future, particularly by those hackers without the skill to manage more sophisticated attacks (Lesser, *et. al*, 1999: 41; McClure, *et. al*, 1999: 340-

341). This might apply to nations who are "growing" their military skills in IO, without hiring outside expertise. It is not meant to imply that these nations do not have citizens with high levels of computing skills, just that few of them may be members of the military currently. This concept would apply more to developing nations.

Hackers with medium skill levels possess a sound basis in hacking. They are still expanding their skill set, often using past exploits or mentors to improve. Information processing skills and their approach to hacking are still expanding (Chantler, 1996: 126). Chantler, and those he surveyed, believe the majority of hackers belong in this category (Chantler, 1999, 113).

Expert hackers have an extremely high skill level (Chantler, 1999, 113). Their approach to hacking tends to follow a structured problem solving methods, and they possess a wide range of knowledge in computing (Chantler, 1996: 126). This group is often referred to as the "elite". Chantler's survey respondents estimated that only 20% of hackers reach this level (Chantler, 1996: 113). It is interesting to note that all of the respondents placed themselves on this category. They felt expert status consists of knowledge, renown (prestige), and service to the hacker community at large (mentoring, sharing knowledge) (Chantler, 1996: 113). These expert hackers may also use lower level hackers as a force multiplier or as "drones". The expert would provide the tools, techniques, and targets for the underlings to attack. PSYOPS or perception management may convince hackers to attack targets, even though they are not members of the group (and may not even support the group) initiating the attack.

3.4.2. Aspects of Teamwork

Taylor discussed how many hackers, who are not members of formal organizational structures, choose to work in informal teams (Taylor, 1999: 60). These teams pool resources and expertise to target larger, more complex systems or to speed their efforts. Most members have a given specialty area or system; teams form to meet the needs of a specific hack. The fluid nature of cyberspace, with no locational restrictions on group membership, readily supports these teaming arrangements. The US Air Force has similar flexibility inherent in its "reachback" approach to many formerly deployed mission areas. Expertise is "tied in" from wherever it resides, and the group may never need to meet "in person".

The fluid nature of teamwork in hacking groups may make these groups, as a whole, harder to profile, especially in the case of modern day terrorist organizations (reference Sections 2.1.5 and 2.1.6). However, when one considers the specific group of interest, the situation may not be as foreboding. These groups would consist of, in whole or part, members of the military, their civilian counterparts, and hired contractor support. As such, they might be physically collocated by higher-level command, or could be seen as tied together by that country's equivalent to the United States MII. However, one cannot assume that this will always be the case.

Additionally, as teams work and train together, common tools and techniques may begin to provide a "hallmark" for specific groups. Mentors or specific training philosophies may also contribute to identifiable aspects of attacks. This would be similar skills and methods learned in terrorist training camps.

Mercenaries, or equivalent "hired" talent, present an interesting dilemma. Mercenaries as such are not allowed by the laws of war, and may choose not to follow these laws or other international agreements (African Business, 1997). If hired as a team, their actions may only tangentially correspond to the way an "in-house", traditional military team would operate. Information as to the presence and identity of such a group would be necessary to properly model such a nation's hackers.

This detail of the Skill and Teamwork factor is interrelated with *Tools* and *Training*, as well as *Leadership, Doctrine*, and *Policy.*

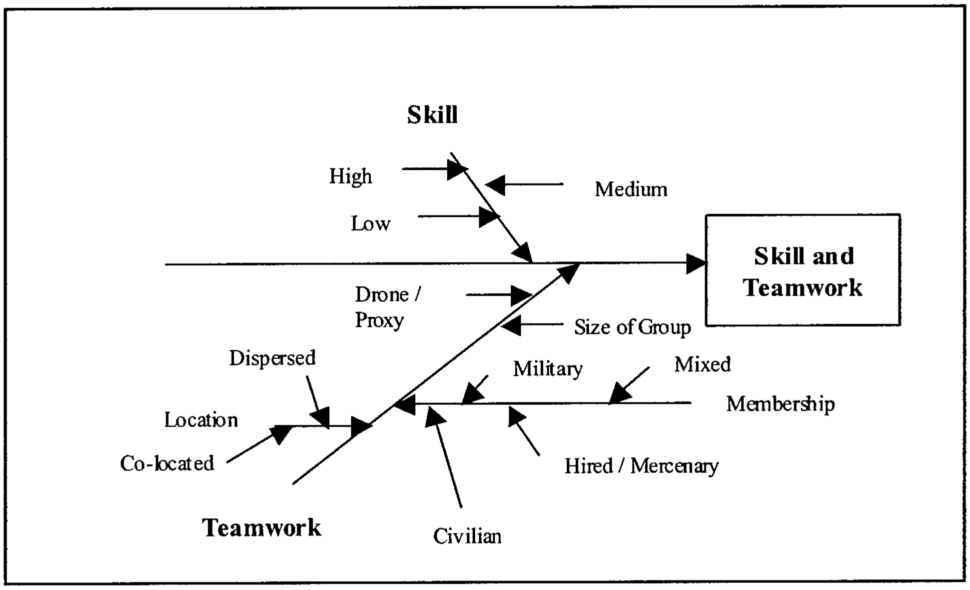


Figure 3-7 Skill and Teamwork

3.5. Hacker Tools and Training

The intent of this factor is not to list every type of tool a hacker might use. Such a list would be of limited practical value as these tools and techniques are constantly changing. McClure, Scambray, and Kurtz detail many of the more common tool and technique types in their book and on the related website http://www.hackingexposed.com (McClure, *et. al*, 1999). Both the book and website provide a broad list of references and Internet websites. A similar reference is Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network by Anonymous (a hacker). Some types of tools, such as social engineering, will be addressed, since their presence can be more easily detected, and can provide information on the group or individual behind the incident. This factor is interrelated with Individual *Skill* and *Teamwork*, and *Leadership, Doctrine* and *Policy.*

3.5.1. Tool sets

One of the first things to remember when addressing the tools hackers might use is that the US can no longer assume it will have the edge in the technology race. Many countries can purchase the necessary equipment and hacking skills required to hack at an elite level. This is one key reason why IO is seen as an asymmetric approach to war. In fact, the bureaucracy inherent in military acquisition processes could be seen as a limiting factor.

There are two basic types of tools that can be used to hack – those that are "published" (generally available) and those that have been created by a group or individual for their own use. Hackers with only limited expertise are confined to the published tools. More elite hackers might use either set depending upon the circumstance. In some cases they might wish to blend in with more traditional hackers (script kiddies, random individuals interested in military systems). This would most likely be the case for long-term intelligence preparation of the battlespace (IPB) efforts. These tools, since known, might however increase the chances of the activity being detected. Even if it is detected, if it does not appear suspicious, it may not be greatly explored due to current limitations on tracking incidents to overseas servers.

Tools that have been created for specific situations are generally much harder to detect. These are the attacks that are rarely, if ever, noticed. These tools require the highest levels of computing skill, and generally must be tailored to the specific target system. The intent behind the tools might be to plant trojan horses, fishbowls, or backdoors into a system in such a way that they can be used in the future for easily launching a concerted IW attack.

Social engineering has been said to be one of the most effective hacking tools. All of Chantler's survey respondents prided themselves in their ability to obtain vital information, to include user names and passwords, from unsuspecting users (Chantler, 1996: 115). Social engineering, which can be seen as efforts at PSYOPS and perception management, refers to using social interactions such as phone calls to obtain information on a target system (Chantler, 1996: 134). Use of telephone calls and email allow a hacker to gain information from a distance. Typically, hackers pose as service personnel, such as computer support technicians. Activities might also involve posing as a security guard or cleaner in order to search for hidden passwords or to "shoulder surf" users typing in their information. This requires that the hacker visit the victim in person. The ability to lie well, act well, and good communication skills are the only requirements (Denning, 1999: 111). Another form of social engineering would be planting a member of the IO cell as an insider. This could occur at those target locations that make use of contractor support, either on a normal basis or for more limited projects. This would pose the most risk, and require the most effort on the part of the hackers.

The last two specific tools to be addressed are the use of rogue code and DoS or DDoS attacks. There are many forms of rogue code, such as viruses, trojan horses, mimic programs, and worms.

Viruses are pieces of code that attach themselves to other programs. Whenever the program runs, the virus runs as well (Denning, 1999: 269). These bits of code can be spread to any system that comes in contact with an infected system either through network connections, e-mail, or via diskette. According to Denning's research, several nations have begun to explore viruses as a method of offensive IW. A 1995 report from the US Defense Intelligence Agency, cited by Denning, stated that Cuban had a program in place to develop viruses with the goal of infecting US civilian computers (Denning, 1999: 275). The report also stated that, prior to the 1991 coup attempt in Russia, the KGB had been developing viruses for use in times of war or crisis. Russian nationalists have suggested that viruses could prove a useful foreign policy tool (Hoffman, 2000). Vladimir Zhirinovsky was quoted in a *Washington Post* article as having said, "Let us put viruses into their secret programs like we did recently, and they will not be able to do anything." (Hoffman, 2000).

Hackers once looked down upon virus writers, but are now learning from their techniques and even combining forces. Many of the motivations given for virus writers are the same for hackers (Denning, 1999: 274-275). An example is the use of viruses to launch a DDoS infection, or to install rootkits or back doors (Rouland, 2000). Chris Rouland, the Director of X-Force (a computer security firm) also predicts that virus attacks will become more coordinated and specifically timed, and that they will target defense systems (Rouland, 2000).

A trojan horse program is one that pretends to perform a useful function, but also performs code in the background without the user's knowledge (McClure, *et. al*, 1999: 132). Its basic purpose is to gain access to an information system or resource (Denning, 1999: 259). Often the background code is malicious in nature. It may also involve alteration of computer programs to perform unauthorized functions (McClure, 1996: 128).

Mimic programs lead victims into believing that they have a valid hardware problem. They may also be written to mislead a user into giving away their user name and password (Chantler, 1996: 128). The code presents what appears to be a normal 'log-on' screen; however, it is set up to pass the account information to both the normal log-on program as well as a hidden directory that the hacker has access to. In this way, the hacker gains the same privileges on the system as the user whose account he has stolen (Chantler, 1996: 128).

Worms are similar to viruses, in that they replicate. However, worms operate independently, and do not require a host program. The host system is not destroyed, but its resources are taken over to support the growth and spread of the worm. This form of malicious code is designed to secretly move through a network, often erasing evidence of its presence, collecting information such as user accounts or documents of interest to the hacker (Chantler, 1996: 129). Worms may also manipulate or destroy data, and may replicate to the point that its network host collapses (Chantler, 1996: 129). Many of the latest generation of worms are propagated via e-mail (Smith, 2000).

Denials of Service (DoS) and Distributed Denial of Service (DDoS) attacks have been discussed previously in Sections 2.3, 2.3.2, and 2.3.3. DoS attacks may be motivated by frustration when efforts to break into a system have failed, for the sense of power it can bring, or a grudge against an organization (McClure, *et. al* 1999: 340-341). While they are often seen as the last ditch effort of a frustrated script kiddie, many authors see them as the weapon of choice for terrorists and nation states seeking to deny access to a system (AFDD 1, 1997: 24; Lesser, *et. al*, 1999: 41; McClure, *et. al*, 1999: 340-341). McClure also feels that DOS attacks will increase due to tools that allow easy launching of DOS attacks, and the opinion that Windows NT/95/98 is a favorite, and readily available target. The goal of a DoS or DDoS attack is to prevent use of a system by bandwidth consumption or resource starvation (McClure, *et. al*, 1999: 344). DoS attacks may be used to force a system reboot so that changes planted by the hacker can take effect, hopefully without the system administrators noticing the changes (McClure, *et. al*, 1999: 340-341). "Many governments have or are in the process of ramping up offensive electronic warfare capabilities that use DoD attacks rather than conventional missiles" (McClure, *et. al*, 1999: 354)

3.5.2. Training

This area includes both individual and team training, and the use of military exercises. Any individual may also engage in self-training in addition to more formal instruction. Due to the attraction hackers have for technology, most will pursue training and improved skills on their own. In this case, any change in the group's style of hacking may be harder to detect.

Individual training is formal coursework or exercises performed at the individual level. Skills learned are not used primarily within the hacking cell to further teamwork, but to improve the skills of the team's members. Since many groups utilize specialized skills of their members, this may involve furthering the expertise of the overall team through training of individual members. This would be similar to specialized skills (communications, first aid) inherent in an infantry platoon.

Team training would be similar in concept to traditional basic or specialized skill training in the military. As such, it may be "behind the times" if it requires the same formal course planning, building, and approval process of other military training courses. Courses by contractor groups, either to military or to military contractors, may be more responsive to changes in technology. IO cells may also decide to take advantage of courses provided by academic organizations, institutes related to computer security, or commercial organizations. While these courses are not meant to train hackers, they often teach hacking techniques and tools so computer security professionals can better guard against them. These courses may provide valuable training for groups building expertise in IO, and may also help develop techniques for "hiding in the noise" of more traditional hackers. It would also provide valuable insight into security vulnerabilities of specific systems.

Group training could also consist of military exercises. These activities are of a larger scale, and tend to involve many types of troops and weapon systems. As IO emerges as a new form of war, it is beginning to take part in these exercises. Currently, IO portions of these exercises are limited, and IO is used as a supporting capability, not as the primary weapon system. This may change in the future, as more countries develop IO doctrine, policy, and plans. These exercises, due to their larger size, may be easier to detect and observe. However, an all-IO exercise may not be as easy to observe, unless high visibility items are targeted. Detection would require that the country's systems of interest can and are being observed, and that successful targeting of systems can be detected.

These team-based training efforts are of interest, since they shape the behavior of those involved. This is why the US puts such emphasis on the concept "train as you intend to fight". If all of any adversary's IO forces have been trained in the same manner with the same doctrine and policy, then they may act in a similar manner when their skills are called upon during conflict. They may share a common set of tools for aspects of the hacking process such as information gathering and vulnerability mapping. While different members may have different specialized skills, their common approach to hacking may make their efforts more predictable.

Hired hacking cells (mercenaries) may not provide this same level of predictability. Mercenaries primarily care about a person's skill level – can they get the job done. They accept trained personnel from many countries (African Business, 1997). Team training would most likely be provided by the mercenary group, and therefore may be less observable. They could, however, develop specific characteristics over time if the same members work together on several operations.

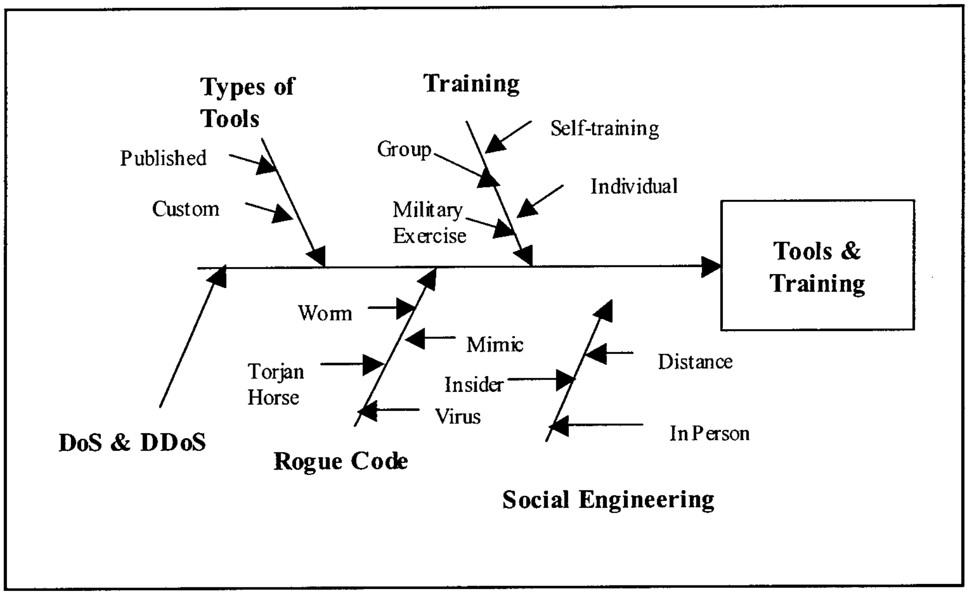


Figure 3-8 Tools and Training

3.6. Intent, Timing and Use of IO

Every action by a military IO group is meant to serve a specific mission or set of missions. Therefore, some aspects of the intent behind an IO incident may be visible with sufficient analysis. Data such as the time of the event, both the data and time of day, and external triggers to the event also provide additional information for the group's profile. Finally, how specific IO tools and techniques are used can provide insight into the intent of the group, as well as the specifics of the group itself.

3.6.1. Intent (Mission)

A single IO or IW attack can serve one or a myriad of missions. US doctrine will be used as a source for concepts of IO mission planning and the intent behind IO operations. This does not assume that other nations will follow US doctrine, but that the doctrine has stood the test of time in traditional conflicts, and is a source for adapting views on IO.

One intent that may provide the bulk of IO incidents is Intelligence Preparation of the Battlespace (IPB). US Joint doctrine holds IPB vital to the success of IO and IW (JP 3-13, 1998: I-18). These efforts in support of IO would require long-term development, possibly longer than traditional operations (JP 3-13, 1998: V-2). IPB efforts would include efforts to locate, identify, and map potential adversary systems and information infrastructures. Sun Tzu wrote, "Both sides stalk each other over several years to contend for victory in a single day." (Huang, 1993: 111).

The growing reliance of US troops on information and information systems provides an asymmetric advantage to an enemy, less reliant upon technology, who can identify US weaknesses. Another aspect of IPB would be efforts to identify a potential adversary in terms of "intent, vulnerability, capability, and opportunity to adversely influence the elements of the friendly information environment critical to achieving objectives" (JP 3-13, 1998: I-16). Finally, IPB would provide a potential adversary with an understanding of US decision making processes and leadership (JP 3-13, 1998: II-12 – II-13).

IO can also be used to shape the battlespace and prepare for future operations prior to initiating a conflict (JP 3-13, 1998: I-4). The idea is to create conditions favorable to achieving ones goals before the conflict escalates into violence (JP 3-13, 1998: I-9). One goal may be to gain Information Superiority over an adversary at the start of a conflict. Once Information Superiority is gained, an adversary would have the freedom to fully exploit their information systems while denying the US access to its own information systems (AFDD 1, 1997: 31). Tools to support the shaping of the battlespace might include placing back doors, planting trojan horses, and developing and/or releasing viruses designed to affect the target systems. A final tool could be the development of DoS or DDoS tool, along with the capture of drone computers to launch the attacks.

A third intent might be deterrence. In this case, IO may not be conducted so much as capabilities are "advertised". Again, JP 3-13 postulates that IO may have its greatest impact as a deterrent, or during the initial stages of a conflict (JP 3-13, 1998: I-3). Deterrence is based upon posturing, maintaining, and exercising forces with sufficient capability to hold at risk a broad range of targets, as well as having the intent to use those forces if efforts at deterrence fail (AFDD 2-1.5, 1998: vi). IO and IW can have a psychological effect far greater than actual physical effects. Threats to cripple or destroy and enemy's key infrastructure may serve a country's objectives more than an actual attack. However, without actual use, there may be a question as to the effectiveness of IO.

The attack of one system cannot, necessarily, be construed as the intent to attack that specific system. Instead, the true intent may be to "hop" from that system to one it is connected to, or to use the conquered system to attack another target. One example is the use of a large number of computers as "drones" when carrying out a DDoS attack. This is part of what makes tracing an attack to its true source so difficult. These attacks could be seen in the light of "primary" and "secondary" targets. Similarly, the intent may be to achieve a "cascading effect". Each successfully hacked system may be linked to a wealth of other systems that are now more vulnerable due to "peer-to-peer" relationships between the systems. Viruses and worms present a clear case of cascading effects, as they are rapidly spread throughout a network. Finally, the intent could be one of creating a synergistic effect, such as operations combining IO with more traditional operations (JP 3-13, 1998: II-3). A synergistic effect may also occur when IO and IW achieve strategic, operational, and tactical level objectives simultaneously.

IO and IW have the unique capability to achieve multiple levels of objectives at the same time. At the strategic level, IO seeks to impact political, military, economic, and informational elements of the enemy's power (JP 3-13, 1998: I-2). Operational level IO supports operations at the campaign level, focusing on adversary forces or combatant commanders (JP 3-13, 1998: I-2, I-10). Finally, tactical level IO involves specific actions to affect an adversary's information and information systems that are directly related to the conduct of military operations (JP 3-13, 1998: I-3). Together with air and space power, IO has added strength and flexibility in that it does not require the achievement of tactical objectives before operational and strategic level objectives are pursued (AFDD 1, 1997: 13). Table 2-5 Air Force Information Operation Goals provides examples of goals at each of the levels.

3.6.2. Timing of Actions

Some actions may be in response to an external trigger. They could then be predicted as a response to an act of aggression, the imposing of sanctions, or other world events. Whenever the US is active in the international world, there is the possibility of adverse reactions from those nations whose goals and objectives are in conflict with ours. The accidental bombing of the Chinese Embassy in Kosovo could be used as an illustration of Chinese hacker reactions to external triggers (Thomas: 12). In addition, Israeli and Palestinian nationals have been waging a hackers' war against each other's government computer systems and websites in the last several months following problems in the Middle East peace process (Ackerman, 2000; Associated Press, 2000; Gentile, 2000).

Other actions could constitute a "first strike" in a new conflict. JP 3-13 states that the strength of IO and IW may be its use in the early stages of an operation or as a deterrent (JP 3-13, 1998: I-3). If the attack is small, meant to prepare the battlespace of finalize IPB, it may go unnoticed. Larger actions, meant to cripple systems or deny access to vital information will be harder to camouflage. However, aspects of stealth may be involved – the conflict has begun, but the adversary does not wish this fact to be known.

3.6.3. Use of IO

One of the first uses of IO supports IPB as well as preparation of the battlespace and actions that can be construed as more traditional attacks (CNA, launching of viruses). This use involves tailoring attacks so that they hide in the normal "noise" seen on a network. The goal is to avoid detection, both during the operation or later when system administrators may notice evidence of actions. If the operation is noticed, the attacker wishes to appear as a script kiddie or another "run-of-the-mill" hacker, rather than as an agent of a foreign nation. Examples of when this would occur are during ping sweeps to gather intelligence on systems, or when an adversary is mapping system vulnerabilities.

Additionally, some low-level attacks may be a way of testing new capabilities prior to actual conflict. Again, this may occur most often with rogue code (viruses and trojan horses). In general, those testing these capabilities would try to ensure the operation went unnoticed. This may involve using civilian or non-military government targets. Overall, most adversaries will not wish to "tip their hand" by providing information on IO capabilities until the situation requires that they do so. This relates to the concept of surprise, one of the principles of war (AFDD 1, 1997: 20). While some capabilities are made known for their inherent deterrent value, others are hidden so that they can be used to best effect.

IO and IW support other principles of war as well. These operations provide unique ways of concentrating mass on enemy targets, with little exposure of troops to the hazards of war. Forces need not be co-located; instead, they can wait to combine forces at the target (AFDD 1, 1997: 16). The interconnected nature of computer and communications networks also allows a wide range of maneuverability, forcing an enemy to react since he does not know from what direction an attack will come. The flexibility, versatility, and speed of IO allow the simultaneous application of mass and maneuver (AFDD 1, 1997: 17).

IO can also act as a force multiplier when supporting more traditional operations (JP 3-13, 1998: VI-2). It may also be the supported operation when IO provided the main effort against the adversary, but other capabilities are required (JP 3-13, 1998: VI-2). Finally, during operations such as IPB, IO may serve as a stand-alone operation. This is not to imply that efforts such as open source collection of information does not support IPB, but rather that such collection may not solely impact the success of the IO-based collection of information.

Finally, IO and IW can be utilized for its inherent capabilities (PSYOP, Military Deception, and CNA) as defined in

Table 2-2 Key Military Capabilities. PSYOP, and the related concept of perception management, involves actions to influence emotions, motives, reasoning, and behavior of the enemy; the enemy's will to fight (JP 3-13, 1999: II-3 – II-6). This may involve enemy efforts to influence US leadership, but also the American public. Military Deception efforts seek to plant inaccurate information or impressions in the mind of the enemy (JP 3-13, 1999: II-3 – II-6). Again, the minds of the American public could prove a valuable target. Other targets would include releasing information that would mislead US decision makers in the assessment of the enemy's capabilities or intent. The third capability, CNA, specifically involves denying access to, corruption (or deception), destruction, or compromise of vital information. It may also involve similar actions against the computer systems on which the information resides (JP 3-13, 1998: GL-5). Examples of these threat areas are provided in Table 2-4 Information Warfare Threats.

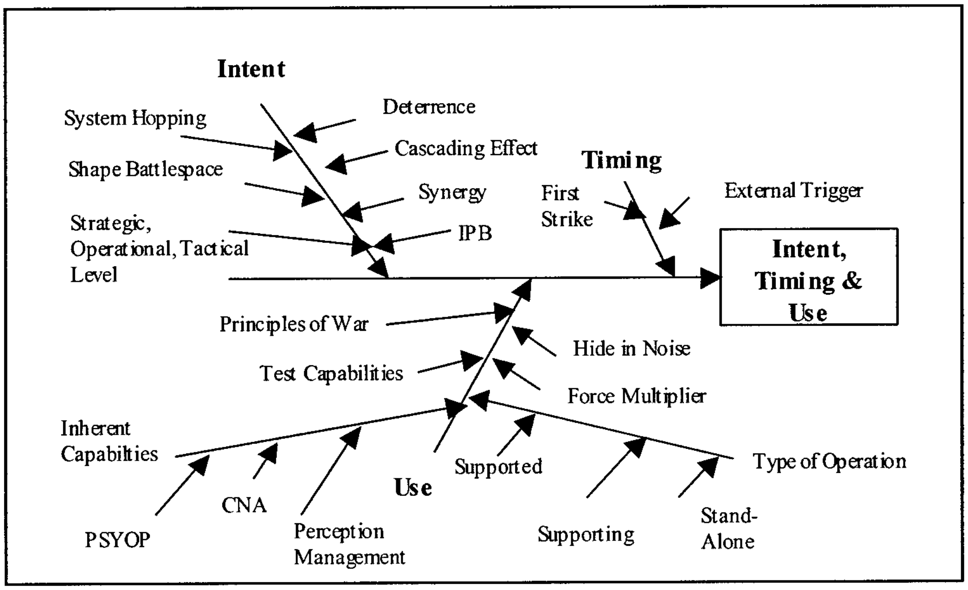


Figure 3-9 Intent, Timing, and Use of IO

3.7. Cultural Impacts

Technology provides a wealth of options for IO efforts. Each country and group utilizing the strengths of IO does so in its own way. Cultural aspects of the country and its people, as well as their shared history, influence the political, social, and military actions of the leadership and general populace. The concept of culture holds that some aspects of a group's character will be the same. For example, in recent months, Israeli and Palestinian nationals have been waging a hackers' war against each other's government computer systems and websites (Ackerman, 2000; Associated Press, 2000;Gentile, 2000). While carried out by the general populace, at least in part, this example provides insight into cultural affects on the type, timing, and use of hacking. The incidents are traced to long-standing arguments of land rights, access to religious sites, and feelings of nationalism.

3.7.1. Nationalism and Patriotism

Feelings of nationalism, ethnicity, and patriotism can provide motivation for military hackers, much as they provide motivation for the all-volunteer United States military. These motivations may inspire hackers to join the military even though higher salaries, better equipment, and better benefits may be available outside the military.

Another area of culture to explore is the "personality" of a nation. For example, the US might be seen by some as a "technology junkie", or as a nation that cannot delay its gratification (keeping up with the Joneses). Therefore, adversaries may see targets in the US NII, GII, and MII that have no equivalent in their own country. The "Y2K" scare in the US may give an adversary an idea of using denial or destruction of access to technology as a PSYOP target against the general public, as well as denying the military access to many military systems that depend upon technology. On the issue of delaying gratification, adversaries may feel that the US is very direct in its actions. Someone who cannot delay gratification may miss better opportunities in the future in order to obtain near-term gains. Conversely, someone who is willing to delay gratification may take actions that appear harmful or less than desirable in the near-term so that a better future is shaped.

3.7.2. Paradigms and Perspectives

Cultural paradigms and perspective color a nation's views of itself, as well as the picture that other nations have of it. JP 3-13 warns of the need to consider cultural perspectives in analyzing a potential adversary or their actions (JP 3-13, 1998; II-12-II-14). This area also affects how one would evaluate the adversary's leadership, doctrine, policy, and potential actions.

3.7.3. Religion

Religion is another key cultural issue. This extends to both the religion itself, as well as to specific religious sects in some cases. Culturally diverse nations such as the United States and the United Kingdom may not have as religious an aspect to their IO organizations as those nations which have a primary, and active, religious nature to their cultural identity. Religious zealots could provide a ready force multiplier if a nation state can convince them, either openly or through PSYOPS, to serve as "proxy" cyberwarriors.

3.7.4. Cyberculture

Hackers may also be seen as members of an additional culture, that of the computer world. This could represent a sub-culture or microclimate to be explored. One respondent to Chantler's survey described cyberspace as "an information world created by technology, in which the mind has the freedom to decide what role its owner should play" (Chantler, 1996: 141). As discussed by Taylor, this culture is very fluid (Taylor, 1999: 30). It evolves at the speed of technology, has an ever changing and hard to quantify membership, and is not bound by borders, language, or location. In some cases, the ties of "cyberculture" and the more traditional culture to which a hacker belongs may come in conflict. This issue must be considered in a profile. It may not be clear whether a hacker has stronger cultural ties to the other members of his IO group, the hacker community at large, or his / her country of nationality. The strength with which a hacker is motivated by peer recognition may provide insight into the specifics of cultural ties. Mercenaries may provide an interesting challenge to profiling efforts, as the country for which they are working may not hold strong cultural ties.

Renfro, in his study "Modeling Individual Behavior", identifies three key concepts in exploring cultural influences. These are Moral Understanding (religion, and relativist / universalistic), Legal System (value of human life), and Political System (Renfro, 2000: 12).

3.7.5. Morality

The influence of religion has already been discussed. The concept of relativistic versus universalistic reasoning deals with issues of right and wrong. Someone who is relativistic looks at right and wrong purely in the context of the current situation perhaps influenced by inclusions of bystanders viewpoints. In contrast, a person with a universalist outlook believes in universal concepts of right and wrong (Curphy, Hughes, and Ginnett; 171). An example is a true conscientious objector – a person who believes it is never "right" to kill another.

3.7.6. Legality

The influence of the legal system can also be seen in relation to hacking. Governments at all levels are passing laws against hacking. Taylor discussed three issues that relate to the success of legislation against hackers, which were summarized in Section 2.2 along with other legality issues. At a more serious level, a hacker's views on issues of legality may impact target selection. Some IO targets, such as communications lines, may potentially result in loss of life, for example due to denial of access to emergency 911 call systems. A hacker with little regard for human life may not worry about the potentially cascading effects of his / her attack. This issue is also addressed in the factors of Intent and Leadership, Doctrine, and Policy.

Renfro's third area of cultural influences, Political System, deals with decision makers and those that might influence them. As such, it is addressed in the factor of Leadership, Doctrine, and Policy.

3.7.7. Psychological Theory

Where specific information is available on a hacker's culture, both in the traditional sense as well as that of "cyberculture", psychology may provide additional levels of detail for the profile. Section 2.4.3 presents the theories of Rotter, Bandura, and Lewin, all of which specifically consider the role of the environment in shaping an individual's motivations and actions. Use of these theories in a specific profile would require significant expertise in the field of psychology. One potentially useful tool requiring such expertise is the Thematic Apperception Test (TAT), which successfully describes British economic growth over a 350-year period (Arkes, 1982: 277). Created as a method of assessing the need for achievement, a TAT test consists of an individual creating a story around an ambiguous picture (Arkes, 1982: 252).

In the case of societal trends in achievement, writings about the same general topics were compared across many years. Some experts question the validity of the TAT to measure motivation (Arkes, 1982: 286), based upon studies where need for achievement does not predict well a given measure of performance. Atkinson, one of the developers of achievement theory, defends the theory with Yerkes/Dodson's law (Arkes, 1982: 287). This states that people with a low need for achievement do better on hard tasks, while people with a high need for achievement perform better on an easy task.

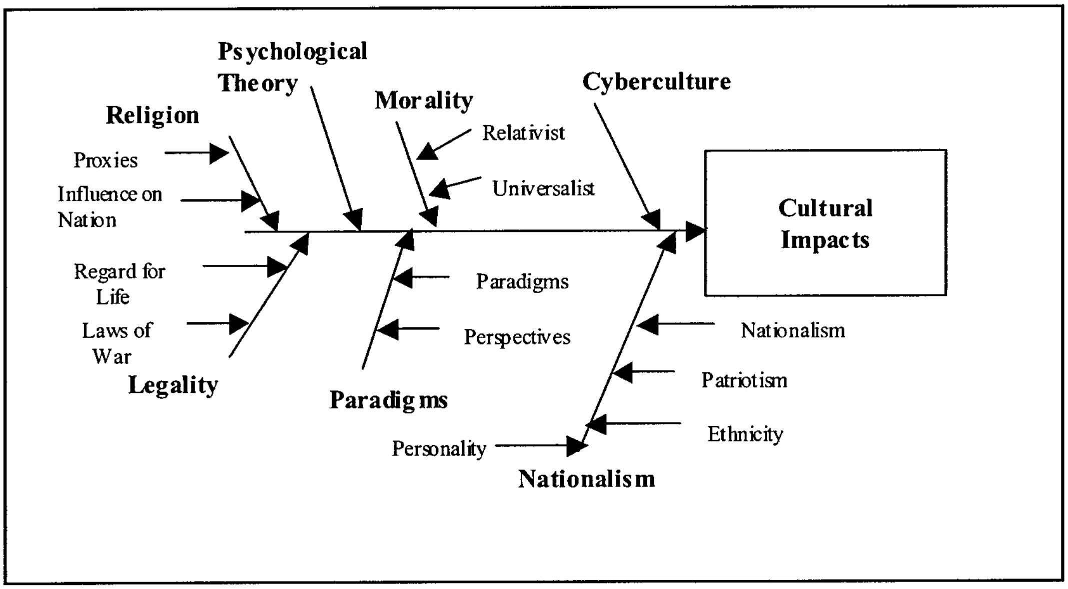


Figure 3-10 Cultural Impacts

3.8. Leadership, Doctrine, and Policy

The organization to which a hacker belongs may have an effect upon approaches, actions, and tool use during an actual hack. Each nation has its own leadership, leadership style, doctrine, and policy. The United States DoD and AF will provide a basis for this aspect of the malicious hacker framework. JP 3-13, AFDD 1, AFDD 2-1.5, and AFDD 2-5, discussed in Chapter 2, will serve as key references.

3.8.1. Leadership

The quality of leadership varies from individual to individual. However, the degree of responsibility and autonomy given to a specific level of leadership and / or branch of military service for a specific nation can be estimated. This aspect explores the structure of the IO cell and its chain of command.

One of the first areas to be explored is the adversary's decision making processes. Are they slow moving, and/or dependent on information technology for collection, analysis, and dissemination of intelligence products? If so, then key influence points, possibly in terms of PSYOPS, Military Deception, or CNA, would be those systems that support the decision makers.

Additionally, is authority for operations centralized or decentralized? A long, formal approval process for IO or IW may limit the effectiveness of the operations. Just as airpower's strengths and flexibility were limited in the US until the Air Force was established as a separate service, if IO cells are controlled by commanders with limited knowledge of their capabilities their operations will primarily continue as supporting efforts. In this case, traditional "hard kills" of systems may be preferred to the less substantiated power of CAN or other IO approaches. The flexibility of IO to react at great speed, limited only by human keystrokes and communications bandwidth, may also be restricted if specific actions must be approved by higher command.

Berger presents the case for decentralized, networked organizations (Berger, 1998: x). Decentralization has the added benefits of encouraging information sharing across lines of authority and passing authority for operations to as low a level as possible (Berger, 1998: 25). Organic (networked) organization structures are more robust in environments experiencing large amounts of change or uncertainty, require little formal coordination, and encourage innovation (Berger, 1998: 33-35). All of these characteristics would benefit a nation involved in conflict. Thus, a decentralized approach to the IO command chains would provide the least impediment to IO's strengths.

A more centralized command structure would be easier to influence and to target. A traditional hierarchical approach to control and organization of IO capabilities, tied with strict adherence to current doctrine, can breed predictability (Berger, 1998: 98). Knowledge of the enemy's command structure and doctrine is vital, then, to understanding how that country will approach and implement IO. On the other hand, if a nation's doctrine allows autonomous action when communications are lost, striking the C4 system might actually speed a foe's response time.

To better understand the enemy, one must also explore issues of command and control. This not only involves IPB aspects of locating and identifying potential systems and infrastructure, but also exploring how leadership, advisors, and units are connected to each other both formally and informally. Determination of who is involved in command and control processes will help isolate viable influence points as well as most suitable targets for specific operations when the US decides to act or respond to enemy actions. Again, if the enemy has developed a networked IO structure, then the most effective lines of command and control may be hard to detect, or their lines may be blurred. However, the goal of profiling the leadership aspect of and enemy's IO organization is to better understand thought processes, approaches to operations, and lines of command and control.

Finally, the issue of leadership should also be addressed with respect to the use of hired IO expertise (the concept of mercenaries). Mercenary groups must rely heavily on trust in both the individual member and, most especially, the leadership. Mercenary leaders depend upon charisma, strength, and skill. While they may not be the most skilled at a given task, the group as a whole perceives them as having been proven "the best" overall (Lavadour, 2001: 60). While the same may not hold true for the formal leadership of a military contractor, within the functional IO cell they provide, this may still hold true. If this is the case, the most effective influence point is to cast doubt upon the leader's ability or trustworthiness.

3.8.2. Doctrine & Policy

Basic doctrine is adapting to the unique capabilities of IO. Doctrine provides overall guidance on the use of military capabilities to meet national objectives. Policy can be defined as doctrine put into practice. The specifics of a situation influence how doctrine is implemented to meet specific objectives in a given situation. Those developing doctrine may find themselves behind the curve of rapid changes in the field of IO. When observing an enemy's doctrine, one must question whether operations plans have moved beyond current published doctrine. Many of the concepts explored in this factor have been discussed previously.

First, a potential adversary's doctrine should be explored for statements regarding how the country sees that IO will be tempered by the laws of war, as well as international law and conventions. These concepts were explored in Section 2.2. Specifically, are some actions (rogue code, attacks on financial markets) weighed in light of their possibly indeterminate or cascading effects? Many of the specifics of more damaging IO capabilities might not be mentioned, so that capabilities remain hidden until they are most needed.

Next, how are IO mentioned with respect to deterrence? This concept was previously developed as part of *Intent*, *Timing*, and *Use*. Again, US doctrine postulates that IO may have its greatest impact as a deterrent, or during the initial stages of a conflict (JP 3-13, 1998: I-3). Deterrence is based upon posturing, maintaining, and exercising forces with sufficient capability to hold at risk a broad range of targets, as well as having the intent to use those forces if efforts at deterrence fail (AFDD 2-1.5, 1998: vi). Other nations have already begun to develop ideas about IO with respect to deterrence. Chinese author Shen Weiguang in a February 2, 1999 article in *Jiefangjun Bao* is quoted by Farris as having written, "Only when we possess the capability to win, and make preparations to win, can we possibly realize the aim of checking the warfare" (Farris, 2000: 38 – 39).

Next, how does the potential adversary's doctrine address the use of IO versus conventional weapons systems? Is IO primarily addressed as a supporting operation, or does it appear to be seriously treated as a stand-alone or supported operation? This could provide insight into how and at what level (strategic, operational, or tactical) IO will be conducted. For example, it may provide an idea of whether US systems and infrastructure will be targeted by CNA versus electronic attack or physical destruction. This could highlight whether information or information systems in the US mainland will be targeted over systems deployed to the area of operations. IO can impinge upon building and sustaining coalitions, as well as highlight the vulnerability of the US homeland in ways not previously seen with traditional operations (Molander *et. al*, 1996: 30).

Finally, how does the adversary's doctrine discuss IO target selection and target sets? Figure 2-2 Examples of Potential IO Targets (JP 3-13, 1998: I-17) presents examples of targets that the US is considering for IO. Are potential synergistic effects explored through the combination of IO with physical attack / destruction or electronic attack (JP 3-13, 1998: II-3)? Is the possibility of bypassing, isolating, or neutralizing a target so that it retains its intelligence value discussed (JP 3-13, 1998: II-14)? Are measures of success identified for IO (JP 3-13, 1998: II-1)? All of these concepts will help place the potential adversary's intent, capabilities, and approaches to use of force in context.

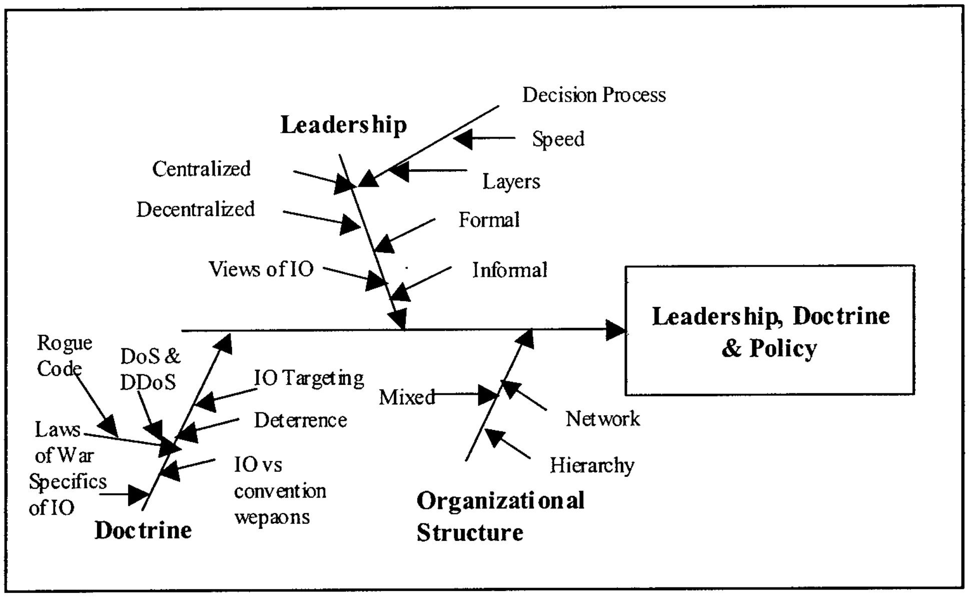


Figure 3-11 Leadership, Doctrine and Policy

3.9. Malicious Hacker Framework

Now that the key aspects that can affect a hacker and the actual hack have been identified, a framework, or scripted profile, has been established to organize the knowledge about a particular nation's approach to IO and to facilitate analysis. Each of the seven factors and their diagram is now assembled into an organized whole in Figure 3-12 Malicious Hacker Profile. As mentioned previously, a strength of the Ishikawa diagram is that the factors need not be mutually exclusive. In fact, areas of overlap provide insight into interrelationship among the factors.

When utilized, available data and expertise on a nation of interest is assembled. Each factor can then be considered in turn. Some aspect of each factor area will be relevant to a group being profiled. It is not believed that all details will be appropriate (or available) in every case. The profile is tailored so that each applicable detail is explored as far as possible or desired, with unnecessary areas being deleted from the diagram. Areas that require more exploration or collection of information can also be highlighted.

The framework, then, serves as a method of consolidating information on a group of interest. It highlights information and intelligence requirements, and may serve to identify sources. Additionally, characteristics of the group are identified along with potential targets, weaknesses, and influence points. This may drive additional requirements for the intelligence community collecting information on the group.

The level of confidence in a given detail can be specified. For example, the belief that a country's hackers are motivated primarily by salary could be weighed against all other motives assumed to be relevant, similar to the way that swing weights are used in VFT. The goal is not to develop a numerical value for motivation, but rather to better understand at an overall level how the hacker is motivated and how he or she could potentially be influenced. For those motivated by salary, efforts might be undertaken to hinder payments of salaries, or bribes might be offered. Additionally, providing levels of confidence in each aspect of the model can provide input to the overall model's ability to describe the group of interest. If provided as part of the diagram, it will highlight the fact that the diagram represents a profile, and not necessarily the "facts" of the group of interest.

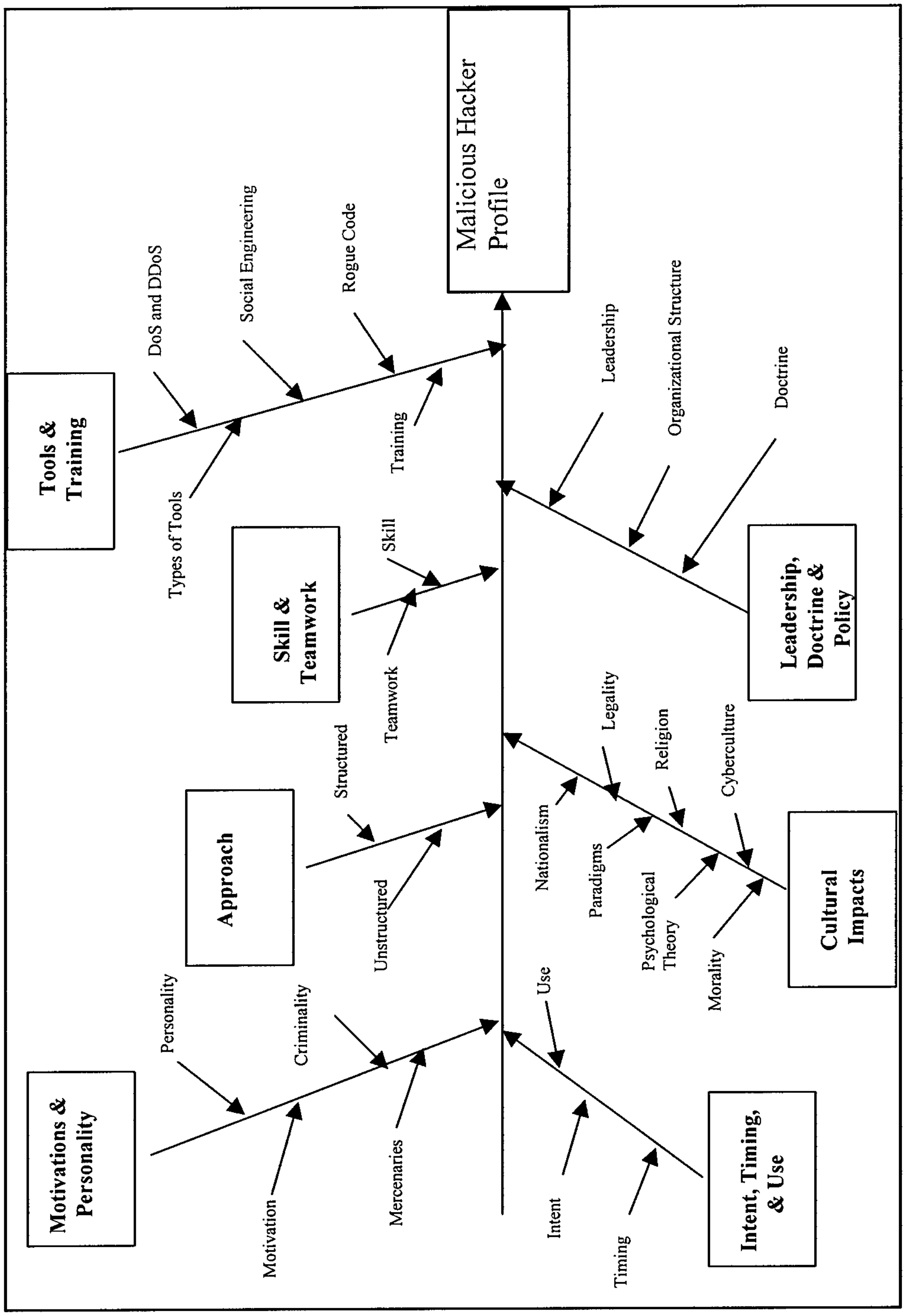


Figure 3-12 Malicious Hacker Profile

3.10. Summary

This section has utilized the review of references in Chapter Two, as well as key model structures, to develop a framework to analyze malicious hackers. Much of the framework is useful in studying the broader classes of hackers, from insiders, to script kiddies, to elite hackers, or even terrorist groups.

Ishikawa diagrams have a unique set of strengths for this type of efforts. The hierarchical nature of the diagram allows for appropriate levels of detail, substantiated by available data. These diagrams are not limited by the availability of quantitative data for each factor and level of detail. Where available, quantitative data can focus efforts on defense measures specific to the area of the data. For example, use of a specific tool or events occurring at a similar time, substantiated by Pareto charts or other numerical tools, can focus defensive IO measures against events using that specific tool or allow greater scrutiny of events during the times of interest.

Chapter Four will use the model developed to study a specific country's IO doctrine, and how state sponsored hackers in that country could be modeled. The case study serves as both a proof of concept and validation of the proposed malicious hacker model.

4. Case Study: Chinese Approach to IO and Hacking

4.1. Introduction

To be operationally sound, the framework developed in Chapter Three must provide a useful analysis of some group or class of malicious hackers. Since the focus of this thesis was on state sponsored hacking, a foreign country with known IO programs and doctrine was needed to serve as a test case. Due to availability of documents and some level of cultural assessment, China has been selected as an appropriate case study.

4.2. Chinese Doctrine for IO

Several sources provide an overall view of Chinese IO doctrine and theory. The Chinese were one of the earliest nations (following Russia) to pursue the concept of IO and IW. By the mid-nineties the Chinese government had discussed the possibility of attacking foreign financial markets (Borland, 1998). Military exercises began to incorporate concepts of computer-based warfare in 1997 (Borland, 1998).

China's long history of actively collecting information on the US and US defense secrets is well known (Gertz, 2000). Sources of information, as early as the late nineteen seventies, include students studying abroad, business people, scientists, and travelers. These individuals were not paid for their efforts, as those collecting the information expect those friendly to China to provide any information freely (Gertz, 2000). Another large source of information is through open source documentation that can be pieced together into "better" intelligence. According to a spying manual recently published by two Chinese intelligence experts, 80% of Chinese spying efforts focus on open source material, with the remaining 20% obtained through illicit means such as the use of agents or electronic surveillance (Gertz, 2000).

4.2.1. Like Adding Wings to the Tiger: Chinese Information War Theory and Practice by Thomas

Mr. Thomas, a member of the US Army's Foreign Military Studies Office, discusses the recent articles and studies published by Chinese scholars on IW in this document. He presents three key results of his analysis (Thomas: 1). First, he believes the Chinese feel a compelling urge to develop IW theory in a manner that is uniquely Chinese. This theory would take into account China's history, military philosophy, culture, and economic situation. Second, Mr. Thomas states that Chinese IW theory is "strongly influenced by Chinese military art" (Thomas: 1). Two examples of this concept are the extension of the People's War concept to IW and the development of a separate "net force" – a separate military branch to address issues of IW. Finally, the Chinese are developing IW theory based on terminology consistent with Chinese military science, which is more in line with Russian (communist) concepts than those of the West. However, Chinese scholars are studying US doctrine and RAND studies to further their own theories and doctrine.

While China is developing this new set of IW theory, it appears that moving theory into practice is proving more difficult (Thomas: 1). China is still developing the necessary infrastructure, both military and civilian, to support their IW theory. This is seen as China's biggest weakness (Thomas: 17). However, Thomas cites a 3 August 2000 *Washington Times* article that states hackers suspected of working for the Chinese government successfully attacked a Los Alamos computer system and gained access to sensitive, but unclassified, information (Thomas: 2). However, China holds a long-standing strength in the formulation of strategic concepts coupled with a focus on long term thought processes (Thomas: 17).

Other targets that appear to be of interest to the Chinese include "information sources, channels, and destinations, and C4I and electronic warfare assets" (Thomas: 2). Primary attack objectives are believed to be information systems linking political, economic, and military installations, as well as US society in general (Thomas: 2).

China believes that it is not of superpower status with respect to its nuclear arms, but that IW, representative of a change in the conduct of warfare, might provide the necessary power to threaten other nations (Thomas: 2). IW attempts to win conflicts in terms of "promptness, correctness, and sustainability", and can attack targets from long distances (Thomas: 2). The area of communications (methods and media) is one of concern for the Chinese due to the strategic nature of their capabilities. Communications can have a deterrent effect and are capable of manipulating the general public, making them a key target during conflicts (Thomas: 8). Adding emphasis to this concept, Thomas states that "Chinese military scientists have studied the ability of IW to affect values, emotions, and beliefs of target audiences, traditional psychological warfare theory, but with IW applications" (Thomas: 18).

The Chinese no longer count military strength in terms of armored divisions, wings of airplanes, or battle groups; concepts such as computing power, communications bandwidth, and system reliability are being addressed as well. Xie Guang, the Vice-Minister of the Commission of Science, Technology and Industry for National Defense, describes (according to Thomas) the three areas of IW as first C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance), then electronic warfare, and finally computer attack and defense methods (Thomas: 7). IW is seen as a way for China to catch up to the West in terms of military strategy and international status (Thomas: 16).

Thomas believes the most far-reaching development in Chinese IW theory is the extension of IW to the theory of a People's War (Thomas: 2). This means that civilians as well as military forces will be involved in IW operations – "the chance of the people taking the initiative and randomly participating in the war increased" (Thomas: 2). The result is a "take home battle" where civilians use laptop computers from home to hack foreign computer systems. Chinese analyst Wang Xiaodong is quoted as having stated, "… an IW victory will very likely be determined by which side can mobilize the most computer experts and part-time fans" (Thomas: 3). "The goal of Chinese doctrine is to unify the concept of People's War with the concept of victory through information." (Thomas: 3) Thomas sees a large, untapped potential in Chinese information engineering and computer specialists (Thomas: 3).

China's reserve forces are adopting this concept of an IW People's War. The People's Liberation Army (PLA) is creating mini IW regiments in some districts (Thomas: 3). A reserve training base for IW has been established, and there are several reports of IW activity by reserve units (Thomas: 3-4). Aspects of this approach could be seen following the US bombing of the Chinese embassy in Kosovo 8 May 1999. Thomas discusses a *Chinese Liberation Army Daily* article detailing a "network battle" between US and Chinese hackers. This article claims that in addition to defacing the home page of the US Embassy in Beijing, Chinese hackers shut down several US political and military website and many civilian web sites (Thomas: 12).

The methods used included DDoS attacks by thousands of Internet users, e-mails loaded with rogue code, and attacks using "hacker tools" buried in programs. The targets of these attacks reflects a common concept held by both Chinese and American analysts – technology is increasing the size of the battlefield even as it is shrinking the size of the world (in virtual terms) (Thomas: 12). Precision targeting of key network nodes (termed acupuncture war by the Chinese) illustrates the ability of IO to attack locations at will, without the requirement for mass troop movements (Thomas: 12).

Several organizations and institutes have been created in the last few years charged with IW training for the PLA. The lead organization, the Communications Command Academy, has published two books – one on Command and Control IW and the other on Technology in IW (Thomas: 8). The first book addresses concepts for building an "information corps" and the principles on which to base Chinese approaches to IW. The second develops trends for basic IW technologies. Thomas states that the academy is "well respected for its IW curriculum that analyzes strategic, operational, and tactical IW requirements" (Thomas: 9). All of the universities, colleges, and institutes reflect the changes in warfare that the PLA sees with respect to IW. The Chinese view IW as a force multiplier and as a strategic resource (Thomas: 9). However, Thomas believes the current level of IW expertise and "culture" of current commanders is relatively low (Thomas: 9).

As a result, training programs are being tailored to the age and position of Chinese troops. High level, older, and somewhat less technically adept commanders receive short duration training (supplemented by other means) geared to eliminating information illiteracy, changing concepts and paradigms, and the application of new IW ideas to future war (Thomas: 10). The Chinese feel that high-technology war demands "a high level of knowledge by commanders and operators, strong psychological qualities, command ability, and operational skill" (Thomas: 10).

Those members aged 30-40 are seen as "transitional-style talent" – the leaders of tomorrow. The focus of their training is on "enhancing their ability to command in IW environments" (Thomas: 10). Training goals include laying a firm foundation in information theory, and gaining a grasp of the requirements, unique aspects, and laws of IW.

Finally, younger members of the PLA receive long duration IW training. It is assumed that they already possess an understanding and appreciation of the modern information-based world. The focus of training at this level is on command and technology. In addition to ideological and theoretical concepts of IW, these students receive advanced instruction in IW methods and develop skill through actual application (Thomas: 10). All training levels addressed basic theory, IW rules and regulations, strategy and tactics specific to IW, information weapons, simulation-based IW training, CNA, and network defense (Thomas: 10). Thomas points out that while articles appear to present China as having superior IW training programs, some reports provide a less favorable picture (Thomas: 10-11). One source states that IW training is not systematic, that it lacks order as well as assessment standards, and its management lacks regulation (Thomas: 11).

The use of military exercises by the Chinese to explore, develop, and institutionalize IW theory and practice has grown since the first IW exercise in 1997 (Thomas: 13). Later exercises extended participation over several regions across China. Exercise objectives have included emphasis on electronic confrontation, discussions on and design of IW training, and campaign-level IW confrontation of forces (Thomas: 15-16).

The establishment of a separate Chinese "net force", which some Chinese scholar's treat as "very likely", is also considered (Thomas: 5). One possible reason for this event is that the Chinese view violations of their cyberspace as important, if not more so due to their secretive nature, than violations of national sovereignty (Thomas: 5). This net force would both defend Chinese systems and information and attack adversary targets (Thomas: 5).

China has a long history of military strategy. One set being re-explored in terms of IW is the "36 stratagems" originally collected over 300 years ago by an unknown scholar (Thomas: 4). One of the overriding issues was the use of deception as a military art supporting the achievement of military objectives, now possibly revitalized as a tactic. Thomas presents five of these "36 stratagems" and provides modern IW interpretations (Thomas: 4).

First, "fool the emperor to cross the sea" – this means hiding the true intent of actions in order to mislead the enemy. Rogue code hidden in e-mail messages or Internet traffic is a modern example. Next, "besiege Wei to rescue Zhao" – attacking something the enemy holds dear if a direct attack is not possible. This would be represented by CNA use instead of conventional operations, and highlights the Chinese intentions to use

IW, potentially against the NII (i.e. the US economy) rather than the MII or GII. Third, "kill with a borrowed sword" – attack using another's strength is a direct attack is not possible. This would be the case when proxies, cut outs, or another country are used to release or spread rogue code. Fourth, "await the exhausted enemy at your ease" – similar to the US principle of war of offensive, this relates to "choosing the time and place of battle". Thomas' IW example is the use of the People's War theory to launch multiple attacks, consuming US computer security resources, and only then launching the true offensive. Finally, the fifth stratagem is "loot a burning house" – use internal conflict to neutralize an adversary's ability to deal with external threats, allowing information to be stolen during the ensuing chaos. Thomas suggests that planting hackers inside Western nations, under the guise of legitimate business people or students, would be a suitable IW application (Thomas: 4). He does not state, however, whether his example is based upon published Chinese views or his own supposition.

4.2.2. Chinese Views on Information Warfare by Farris

Kate Farris provides a thorough open source discussion of Chinese views on Information Warfare, and the caution that must be applied in drawing conclusions from Chinese writings on the topic. China began a military buildup in the 1980s, and evolving concepts of IW provided a strong focal point (Farris, 2000: 76). Additionally, the Chinese leadership was adapting to a changing international scene.

The global environment had changed with the fall of the Soviet Union and the swift pace of Desert Shield / Desert Storm. Additionally, China was dismayed by the growth of democracy in Taiwan, as they believe that China and Taiwan are one nation (Farris, 2000: 76). Some experts also believe China may try to exert more influence in the Asian continent as a result of their newfound wealth and power (Farris, 2000: 77). This may lead to situations where US and Chinese national objectives are in conflict. Therefore, the US should consider how evolving concepts of IW may influence the initiation, duration, and conclusion of such conflicts.

While a discussion of topics by Chinese leadership does not imply intent to act upon one, several, or any of the topics, IW appears to have become a key concept for the Chinese in recent years. However, any result will necessarily have a Chinese orientation that need not directly correspond with American views on IW. Differences in views on IW are a result of different force structures, different military histories, and different experiences (Farris, 2000: 70). This holds true for any two nations being compared, but is still a critical mindset to remember. Farris notes that China sees IW, particularly perception management, as being integral to both military and civilian life, whereas the US treats it as an almost exclusively military issue (Farris, 2000: 70). The US should recognize, in light of the highly interconnected National Information Infrastructure (NII), that "in the information warfare era, the relationship between civilian forces and the war itself will be much closer than ever before" (Farris, 2000: 69).

Farris does not believe it is correct to say that the Chinese are incorporating IW into their doctrine. Rather, IW "precedes, overarches, and encompasses all facets of military doctrine and strategy" (Farris, 2000: 3). Much as the US views IO to be ongoing, the Chinese believe IW and perception management begins before a conflict and continues after conflict ends. While the US acknowledges technology transfer between the civilian and military sectors occurs, for security reasons the Chinese focus solely on transfer from the civilian sector into the military (Farris, 2000: 4). Chinese institutions are being created to incorporate IW operationally from the national level to the system level (Farris, 2000: 4).

According to a 27 April 1999 article in *Biejing Keji Ribao*, the PLA has created a cross-disciplinary doctoral level program in IW at the Communication Command Academy. Sub-disciplines include "information warfare psychology" and "information warfare transmission". The academy has also sent specialists to lecture at military headquarters, units, and service academies (Farris, 2000: 55 - 56).

The Information Engineering University, part of the PLA, was created to prepare professionals for future high-technology conflicts involving IW according to a 17 November 1999 article in the *Beijing Xinhua* (Farris, 2000: 56).

The "National Defense Science, Technology and Information Center" was created to train technical personnel in IW, to establish an IW simulation center, and to study IW theories and technologies. A 15 September 1999 article in *Chung-Yang Jih-Pao* stated one of the center's goals is to attract both young and middle-aged experts from home and abroad (Farris, 2000: 57 - 58).

A simulation center was discussed in the September / December 1996 Zhongguo *Guofang Keji Xinxi*. The center, complete with advanced technical equipment would employ high-technology methods to "create a simulated IW environment" and carry out "training in simulated countermeasures". Expert personnel would be employed to study science and technology problems, demonstrate new equipment, conduct theoretical research, and teach other staff members. Information technology specialists would also be employed to test, demonstrate, and simulate countermeasures (Farris, 2000: 57 - 59).

In an interview for Taiwan Central News, published 31 May 1999, Taiwan's Mainland Affairs Council Vice Chairman Lin Chong predicted that IW would become the top item on China's military development agenda (Farris, 2000: 4). China's tradition of posturing itself as a weaker nation that would be taking on a more powerful enemy leads in many cases to a view of IW as an asymmetrical tool (Farris, 2000: 76).

The Chinese leadership has studied Desert Storm and the more recent conflict in Kosovo. They are upgrading the technological underpinnings of their forces, while also exploring the potential changes such technology may bring to the military structure (Farris, 2000: 7). However, they lack practical experience in IW using high technology (Farris, 2000: 7). Deficiencies identified by the Chinese in their current capabilities include the need to flatten and automate command structures, conduct systems architecture research, link IW to increased combat effectiveness, train personnel in IW, and building a military intranet and extranet according to a 15 September 1997 article in *Zhongguo Dianzi Bao* (Farris, 2000: 8).

To overcome these deficiencies, various Chinese leaders purpose both symmetric and asymmetric responses. Those pursuing symmetric approaches believe China should invest in technology in as many aspects as possible. Detractors point to the fall of the Soviet Union, which sought to meet the US in this manner (Farris, 2000: 8). To an extent, these two views represent two different approaches to IW – indiscriminate attacks versus precision attack (Farris, 2000: 17). The inherent problem with indiscriminant attacks is the imprecise nature of expected outcomes (Farris, 2000: 45). Precision attacks, seen as the hallmark of a symmetric approach to IW, allow a better assessment of outcomes but require more detailed knowledge of the adversary's systems (Farris, 2000:

45). This requires that links be established between IW attacks and traditional combat actions.

According to the 11 November 1999 *Jiefangjun* Bao, at least one proponent of a symmetric approach feels IW must be integrated into other combat actions, and that a conflict cannot be won solely using IW (Farris, 2000: 46). However, China recognizes that it still lags the US in the technology necessary to carry out precision (symmetric) IW attacks (Farris, 2000: 17). Farris believes it is clear that China will pursue both symmetric and asymmetric approaches to IW (Farris, 2000: 49). She bases this belief on the upgrade of China's C4ISR infrastructure, as well as their traditional reliance on asymmetric tactics and the teachings of Sun Tzu (Farris, 2000: 49).

Farris states that some of the proponents of a symmetric approach to IW may be "merely discussing US concepts without applying them to China", rather than have true support for the concepts (Farris, 2000: 9). This further complicates an analysis of a Chinese approach to IW, as one must somehow discriminate between Chinese reviews of US (and other foreign) concepts of IW and how those concepts might or might not be applied to the PLA. To approach this problem, Farris explores the differences and similarities between the US and China using the Six Pillars of IW from JP 3-13.

The Chinese are focusing their IW efforts in areas of traditional strength, as well as on areas of known deficiencies (Farris, 2000: 14). While the US is becoming more reliant on interconnected networks and high-technology tools, the Chinese still rely in part on redundant landline communications or the use of couriers (Farris, 2000: 15). This difference in level of technology dependence in operations could provide the Chinese a level of defense against computer network attack by the US.

Joint Publication 3-13, discussed previously, lists six aspects of IW as PSYOPS, Denial and Deception, Electronic Warfare, Computer Network Attack (CNA), Physical Destruction, and Operational Security (Computer Network Defense [CND]). Farris discusses Chinese views on IW on each of these concepts in turn.

PSYOPS

One of PSYOPS' key components is perception management, which has already been recognized as a traditional concept for the Chinese. Propaganda is a PSYOPS tool that seeks to disseminate information to a target audience (Farris, 2000: 18). Examples can be seen in the news media surrounding any conflict. For China, statements by and documents from leaders in regards to Taiwan and China's "one nation" policy are instances of propaganda. Like IO, PSYOPS begins before a conflict and continues afterward. It serves to affect the minds of the general public and the world at large, to affect the decision making process of the leadership, and may also provide insight into a future enemy's intent (Farris, 2000: 19 - 20). Like IW, PSYOPS can blur the line between the homeland and the theater of operations (Farris, 2000: 20).

Denial and Deception

Key concepts in Denial and Deception are deceiving the enemy as to one's true capabilities and concealment of forces (Farris, 2000: 22). Farris presents the case of the Chinese government's failure to release President Clinton's apology over the bombing of the Chinese Embassy in Kosovo for four days as an example of the combination of PSYOPs with Denial and Deception (Farris, 2000: 23). Farris casts this in the light of perception management, common in both military and civilian affairs in the Chinese culture.

Electronic Warfare (EW)

Chinese views on electronic warfare were greatly influenced by the Gulf War (Farris, 2000: 24). Integration of EW efforts across peacetime and wartime efforts is sought. Long-term surveillance during peacetime would lay a firm foundation for efforts in times of conflict (Farris, 2000: 25). Farris also mentions a single reference alluding to specific EW units (Farris, 2000: 25-26).

CNA

Farris addresses both traditional concepts of CNA as well as Computer Network Monitoring (CNM). CNM, a possible precursor to CNA, involves the Chinese intent to monitor and control Internet traffic for potentially traitorous comments (Farris, 2000: 28-29). This can be seen as an additional form of perception management. Chinese concepts of CNA extend under the broader scope of Information Attack to include covert efforts in support of IPB and overt actions such as polling US public opinion (Farris, 2000: 32). According to Farris, "China openly admits that many of the visiting scientists, students, and other Chinese nationals living in the West collect unclassified data" (Farris, 2000: 36).

Physical Destruction

Chinese authors do discuss this more traditional form of warfare. One approach that is discussed focuses elimination of key nodes and links in both the military and civilian information infrastructures (Farris, 2000: 26).

Operational Security (CND)

Farris found little discussion of Computer Network Defense (CND). She states that this dearth of information may be the result of China recognizing a weakness in this area (Farris, 2000: 37). One military exercise focused on combating computer viruses is mentioned.

4.2.3. "The Revolution in Military Affairs" from Chinese Views of Future Warfare edited by Michael Pillsbury

Michael Pillsbury served as editor on this work, which is published under the auspices of the Institute for National Strategic Studies. This collection of articles by several Chinese military and civilian scholars explores China's Revolution in Military Affairs following the rapid growth of military technology in the Information Age. Authors of specific concepts will be identified. In many cases, US doctrine provides a basis for discussion of changing Chinese doctrine and strategy. Only those aspects of the document relating to IO and IW will be addressed. It is interesting that Mr. Pillsbury notes in his Preface that, according to several Chinese military officers, the top Chinese military strategists never publish openly (Pillsbury, 2001).

Chang Mengxiong addresses "Weapons of the 21st Century". IW is seen as "warfare to win people's minds and boost morale by employing … (media products) … focused on the use and prevention of use of information" (Pillsbury, 2001). The author believes that in the modern age, combat capability is determined by a military unit's information capability. Information superiority will be even more important than, and will be required prior to, traditional land, sea, and air superiority (Pillsbury, 2001). Chang Mengxiong believes that IW is the most complex form of modern warfare, and it will decide the winner of future conflicts (Pillsbury, 2001).

He also addresses the concept of deterrence with respect to IW. While he does not believe that it currently exists, he states that it may appear in the future (Pillsbury, 2001). Even if adversaries are matched in traditional military strength, whichever nation has the advantage in IW capabilities stands the best chance of deterring or winning the conflict (Pillsbury, 2001).

Issues of organizational structure are also addressed. The Chinese have studied the lessons of Desert Storm, and some believe that highly-centralized command structures are unsuited to modern, high-technology warfare (Pillsbury, 2001). The sophistication of modern information systems creates conditions suitable to centralized command at high levels and enables independent combat commands at lower levels. Networked and dispersed command, control, communications, and intelligence systems provide robust, reliable capabilities that are resistant to destruction (Pillsbury, 2001). This will ensure lower level commanders access to the information they need to make decisions about their forces while still adhering to the overall plans of higher headquarters (Pillsbury, 2001). The number of staff levels will decrease, and military organizations will mix high levels of centralization and decentralization supported by the military information infrastructure (Pillsbury, 2001).

Additional concepts addressed by this scholar include the issues of use of simulations and the need for highly skilled personnel. Simulations and exercises, involving a mixture of real and virtual targets and connecting units from multiple locations, will be used by the Chinese to prepare for future conflicts (Pillsbury, 2001). Chang Mengxiong states that the human factor will become more prominent in the age of high-technology warfare. The number of military units will decrease, even as their capabilities increase (Pillsbury, 2001). Warfare will become more mental than physical, and the education and technical skills of the officer corps will exceed that of the civilian sector with respect to information technology (Pillsbury, 2001).

Major General Wang Pufeng is the next author in this work to specifically address IO. His article is titled "The Challenge of Information Warfare". The general also believes that the rapid growth of information technology has lead to a revolution in military affairs. (Pillsbury, 2001). He states that, in the near future, "information warfare will control the form and future of war", and will provide the primary driving force of modernization in China's military (Pillsbury, 2001). Efforts will focus on strengthening "information technology, information weapons systems, and information networking".

The General believes that IW theory will exist as a new theory of war, and must be used in conjunction with Marxist and Maoist warfare theory (Pillsbury, 2001). China's current weakness with respect to Western IW capabilities leads the general to emphasize asymmetric approaches to IW – using inferior equipment to achieve victory over a better-equipped adversary (Pillsbury, 2001). Intelligence Preparation of the Battlespace (IPB) and efforts to shape the battlefield, along with China's defensive capabilities, will determine the progress and outcome of any future wars (Pillsbury, 2001). Just as in US doctrine, the general believes that seizing and maintaining the information offensive (information superiority) may precede, or be combined with a traditional strategic offensive. Efforts in support of this goal would include active offensive information attack and information suppression (Pillsbury, 2001).

It is interesting that the General states the US used computer viruses to destroy Iraqi air defense computer systems during the Gulf War.

An asymmetric approach to IW upholds the traditional military theory of Mao Zedong, and can be said to directly support existing Chinese paradigms of warfare. Major General Wang Pufeng believes that China's military has a strong tradition of flexible fighting methods and nonlinear warfare concepts that form the basis of IW's strength, but currently lacks practical battle experience (Pillsbury, 2001). For the near-term future, China will have to overcome its weaknesses in fielded information systems by focusing on the organization and training of specialized IW troops and the development of IW weapons to raid enemy operations platforms and bases, and to damage or foil enemy offensive operations (Pillsbury, 2001). Changes in doctrine, strategy, and tactics to accommodate the information revolution are seen as a vital task (Pillsbury, 2001).

Finally, the general also stresses the need to cultivate expertise in IW. Operating technical personnel, those sitting before computers and instruments, are seen to be as important as more traditional combat personnel (Pillsbury, 2001). Training and study are seen as the methods to obtain the necessary talent.

Senior Colonel Wang Baocun and Li Fei address more of the specifics of IW in an article entitled "Information Warfare". They see IW as efforts aimed at seizing the battlefield initiative. The five major elements in their definition of IW include: military deception, operational secrecy (OPSEC), psychological warfare, electronic warfare, and physical destruction (Pillsbury, 2001). These are the same concepts addressed in US IO doctrine. Computer virus warfare is included in a broader definition if IW.

IW is also seen to impact general concepts of warfare. The colonels feel rivalry over information superiority will be intense, and that IW will expand the general concepts of warfare. For example, as with other Chinese scholars, the colonels feel primary targets in future wars will be the elimination or control of enemy information systems (Pillsbury, 2001). They believe future wars will be harder to win due to the extended target set, as both the traditional military "material bases" and the information systems must be addressed.

Additionally, the pace of battle will shorten as attacks are launched over communications networks. Combat objectives will evolve from total surrender to limited political objectives (Pillsbury, 2001). The concept of force concentrations will also evolve from ideas of quantity to those of quality. "Force concentrations will occur faster, more precisely, and more often during operations." (Pillsbury, 2001)

Finally, organizational structures will change. Officer corps will consist of more technical specialists, and less of staff and command billets (Pillsbury, 2001). The colonels support the establishment of a separate IW branch of service. The units themselves will be smaller, better integrated, and multifunctional (Pillsbury, 2001).

4.3. Chinese Specific Malicious Hacker Framework

"Therefore we say: By perceiving the enemy and perceiving ourselves, victory thereby has no unforeseen risk." (Huang, 1993: 93)

Sun Tzu stressed the importance of understanding one's enemies and potential enemies in his writings over a thousand years ago. The Art of War is still studied by modern militaries. The ability to expand this understanding to the evolving forms of IO and IW is one of the goals of this work.

The information provided by the open source documents reviewed above will now be used to tailor the basic malicious hacker framework presented in Chapter Three to the specifics of Chinese IO and IW organizations and hackers. Due to the limited nature of this information, the model developed will be more representative of an "average" Chinese "cyber warrior" than a specific individual.

Each of the factors in the basic framework will be addressed in turn. The results of this analysis will then be integrated into a complete profile. The references utilized in this Chapter were first presented individually to enhance an overall appreciation of Chinese views on IW. Details from the various works will be briefly summarized under the relevant model details.

4.3.1. Motivations and Personality

Little information from the references relating to Chinese IW can be construed as addressing Motivations and Personality. What could be found is summarized below.

Chinese Hacker Motivation in General

The only motivation from Table 3-2 Malicious Hacker Motivations that is upheld directly by the references on Chinese IW is that of governmental. A case can be made, based upon the actions of Chinese hackers following the US bombing of the Chinese Embassy in Kosovo, to support feeling of national pride as a part of recognition (Thomas: 12). Overall, one cannot assume that China's hackers are any more or less motivated by the remaining motivations discussed in Section 3-10.

Personality

Similar to other aspects of *Motivations* and *Personality*, no direct sources for assessment of this factor was found in the open source references on Chinese IW.

Mercenaries

No support was found in the open source references to support the use of mercenaries or other hired IW support by the Chinese. Rather, the documentation suggests serious efforts on the part of the Chinese government and military to grow expertise in information technology throughout both the military and civilian sectors (Farris: 2000: 8, 56-58; Thomas: 3-4).

Issues of Criminality

Although some mention was made in the references with respect to laws and regulations regarding the use of IW, specific issues of criminality did not arise (Thomas: 10). However, use of Chinese nationals living within the US to launch a cyber attack against US networks would put the US government at a disadvantage. Currently, US law would treat the issue as a criminal matter, making it hard to pursue any ties the hacker might hold to the Chinese government.

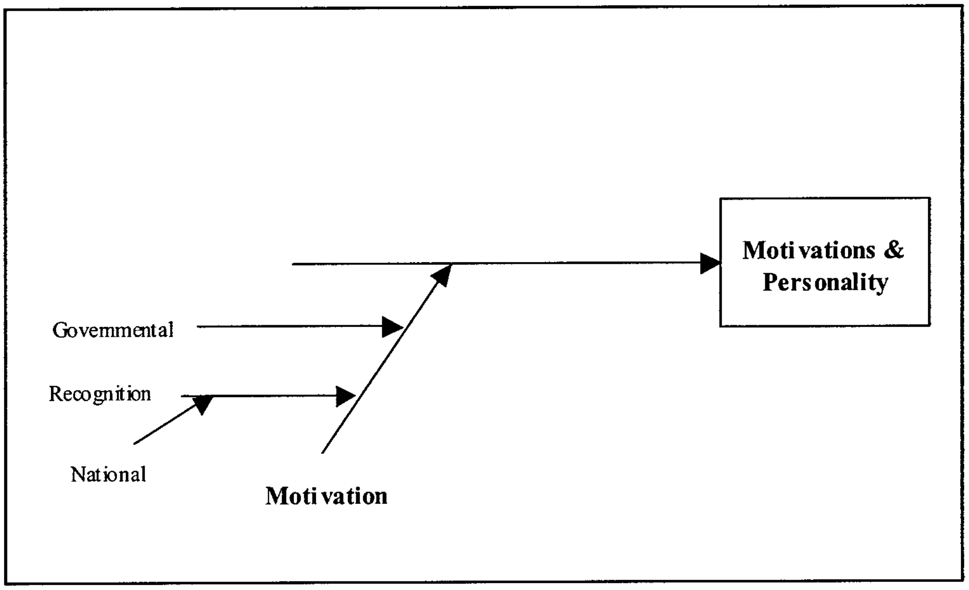


Figure 4-1 Chinese Motivations and Personality

4.3.2. Approaches to Hacking

The two approaches to hacking are structured and unstructured. The references reviewed suggest that Chinese hackers will employ both. First, a case can be made for structured approaches through the development of IW doctrine and strategy (Thomas: 1, 2, 17; various, 2001). This would involve planned activities such as IPB, shaping the battlespace, and CNA.

Unstructured attacks would most likely involve the concept of the People's War – civilian hackers "taking the initiative and randomly participating in the war" (Thomas: 2). This is not meant to imply that many of the civilians are not highly skilled hackers, but that the use of DoS, DDoS, and rogue code in attacks upon US information systems following the accidental US bombing of the Chinese Embassy in Kosovo would indicate the presence of unstructured attacks by Chinese civilians (Thomas: 12). Additionally, the idea of a "take home battle", a Chinese concept cited by Thomas suggests widespread participation by Chinese nationals with a wealth of skill level (Thomas: 2).

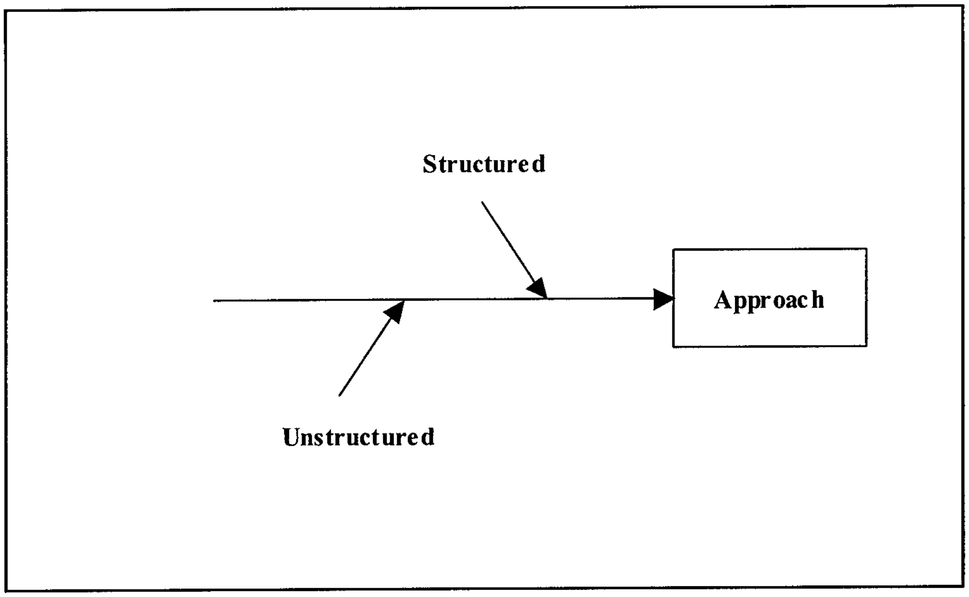


Figure 4-2 Chinese Approach

4.3.3. Individual Skill and Teamwork

The references examined do provide a level of detail with respect to skill levels and the make-up and location of IW teams.

Individual Skill Levels and Talent

The use of civilians as part of a People's War contributes to the skill assessment of an average Chinese hacker. Combined with the opinion of those Chinese scholars that formal training in IW has yet to live up to its potential, hackers will be found at all skill levels (Thomas: 1-3, 10-11). Existence of these schools would lead one to believe that Chinese hacker skill will grow over the next several years, limited only by the pace of information infrastructure development, a recognized weakness of the Chinese military and civilian sectors (Thomas: 17).

Aspects of Teamwork

Specifics of teamwork and how IW units would function were not provided in the open source references that were reviewed. However, the existence of such units, as well as simulations and military exercises supports the idea that IW units will function as teams (Farris, 2000: 56-58; Thomas: 1; Pillsbury, 2001). The existence and training of reserve PLA units would also support this statement (Thomas: 3-4). Use of a People's War concept, and the third stratagem would support the military's use of proxy "cyber warriors" and mixed team membership (Thomas: 2-3, 4). In the context of military exercises, the use of both co-located and dispersed IW units was mentioned (Thomas: 13, 15-16). Finally, the article by Senior Colonel Wang Baocun and Li Fei refers to future units being smaller, better integrated, and multifunctional (Pillsbury, 2001).

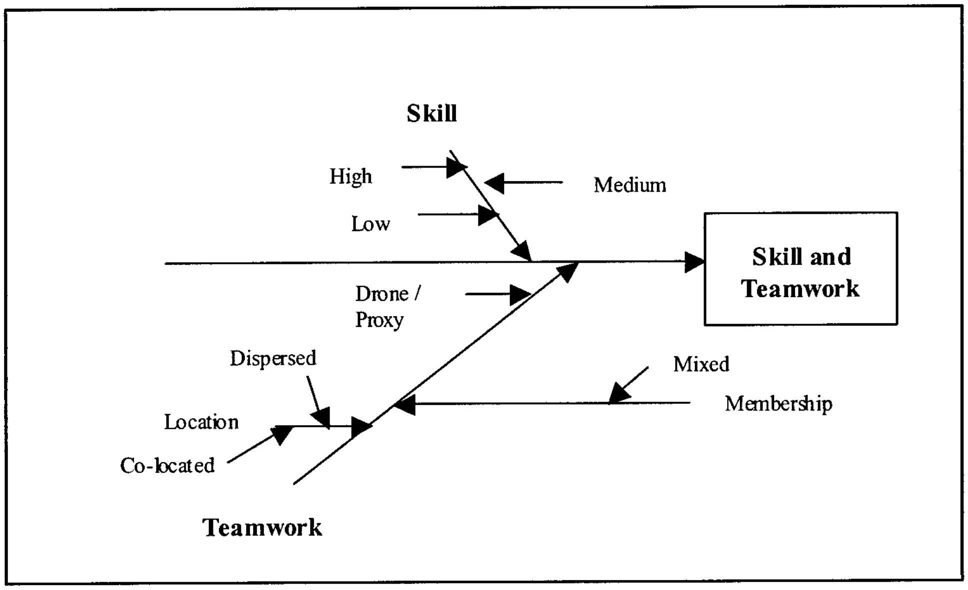


Figure 4-3 Chinese Skill and Teamwork

4.3.4. Hacker Tools and Training

All details of the basic framework are supported by the references on Chinese views of IW.

Tool Sets

The use of both published (readily-available) code and that developed for specific targets or operations is reflected in the People's War concept and specific mention of virus use and development (Thomas: 2-3).

DoS, DDoS, rogue code, and social engineering are all evident in the references (Farris, 2000: 36; Thomas: 4, 10, 12; Pillsbury, 2001). The most common form of rogue code mentioned is the computer virus, followed by trojan horses. Social engineering is mainly discussed in terms of intelligence collection efforts by Chinese nationals (students, scientist, and business people) in foreign countries (Farris, 2000: 36; Gertz, 2000).

Training

Training of IW troops was addressed in several places (Farris, 2000: 25-26; Thomas: 10-11). China has created several formal training programs for all levels of Chinese military and civilian leadership (Farris, 2000: 55-59; Thomas: 3-4, 9-11; Pillsbury, 2001). Training, in the forms of self-training, individual, and group level programs appears to be ongoing. Military exercises, begun in 1997, have continued to expand in terms of doctrine, content, and breadth (Thomas: 13-16; Pillsbury, 2001).

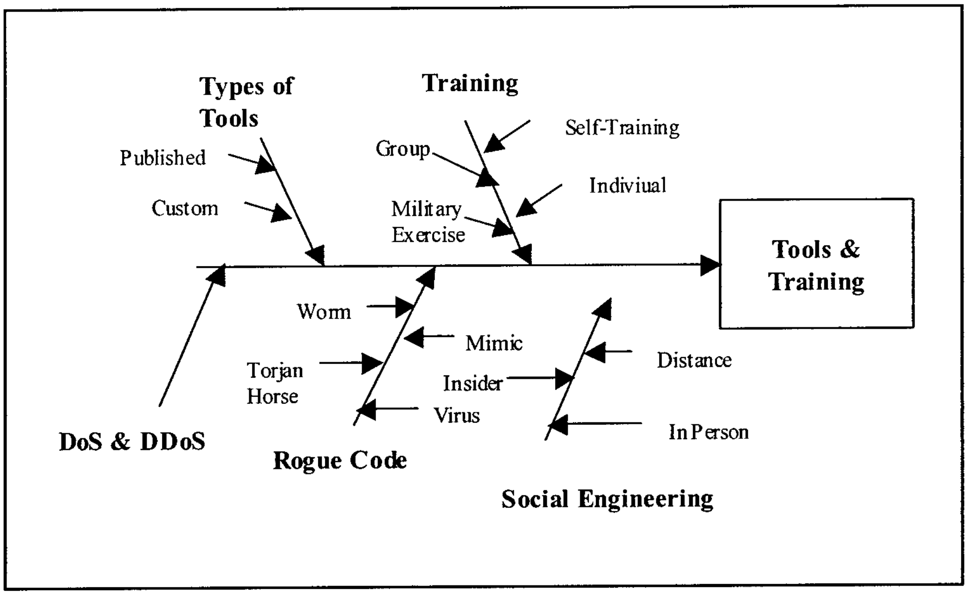


Figure 4-4 Chinese Tools and Training

4.3.5. Intent (Mission), Timing and Use

This factor in its entirety is supported by the Chinese IW references.

Intent (Mission)

Frequent mention of intent or missions of Chinese IW is made in all of the references. IPB efforts (Farris, 2000: 3-4, Gertz, 2000) and Shaping the Battlespace (Farris, 2000: 3-4) are highlighted on several occasions. Additionally, IPB is mentioned as it is supported by social engineering methods (Farris, 2000: 36). Chang Mengxiong specifically discussed deterrence through IW (Pillsbury, 2001). Cascading effects, synergy, and system hopping are illustrated by the Chinese scholars' focus on the asymmetric aspects of IW (Farris, 2000: 8, 17, 4; Pillsbury, 2001). Primary targets are listed as adversary information systems linking political, economic, and military installations, as well as the adversary's society in general (Thomas: 2). Additionally, Chang Mengxiong states that IW is focused on the people's minds – both leaders and the general public (Pillsbury, 2001).

Timing of Actions

The accidental bombing of the Chinese Embassy in Kosovo illustrates Chinese hacker reactions to external triggers (Thomas: 12). The use of IW as a "first strike" capability, or to set the pace of conflict is also discussed in the references (Farris, 2000: 3-4; various, 2001).

Use of IO

The Chinese have begun to adapt existing concepts of IW to their own culture and history (Thomas: 1). Military objectives at all levels are discussed in terms of IW actions, as well as the fact that IW allows targets at the strategic level to be attacked even before operational and tactical objectives have been achieved (Thomas: 17, Pillsbury, 2001). Operations involving IW are seen as being stand-alone, supported, or supporting depending upon the needs of the situation (Farris, 2000: 26, 32; Thomas: 4; Pillsbury, 2001). Two Chinese scholars felt that in the future combat objectives would become more limited and political in nature. There was even some discussion of creation of a separate IW branch of military service (Pillsbury, 2001).

The inherent capabilities of IW in terms of concepts such as CNA, PSYOPs, and perception management, were frequently discussed. Senior Colonel Wang Baocun and Li Fei discussed major elements of IW in much the same terms as US doctrine (OPSEC, military deception, PSYOPs, EW, and physical destruction) (Pillsbury, 2001). This is in part due to the fact that Chinese doctrine and capabilities, along with those of other nations, are rapidly evolving. The capability of IW to have a psychological effect on the values, emotions, and beliefs of adversary audiences was considered by some Chinese scholars (Thomas: 18). Perception management in China is more of a way of life, both in the military and civilian sectors than is the case in the US (Farris: 2000: 70).

The idea of testing capabilities prior to their use in battle may be evident in the alleged penetration of Los Alamos computer systems containing sensitive but unclassified information by hackers working for the Chinese government (Thomas: 2). IW's ability to act as a force multiplier is also addressed – again as part of the People's War or "take home battle" (Thomas: 3).

China's "36 stratagems", which are the equivalent of the US's principles of war, are still seen as valid in the new world of IW. Deception is considered one of its key concepts (Thomas: 4). Other strategies addressed include offensive, surprise, mass, maneuver, and objective (AFDD 1, 1997: 12-21; Thomas: 4; Pillsbury, 2001). The Chinese also consider the use of insider threats so that the resultant chaos facilitates intelligence collection from external sources (Thomas: 4). The first of these stratagems presented by Taylor directly addresses IW efforts that would seek to hide in the noise of normal network traffic (Thomas: 4). Finally, asymmetric attacks, a common idea in Chinese discussions of IW, cold also be seen as a modern interpretation of the principles of war (Farris, 2000: 8, 17, 45; Pillsbury, 2001).

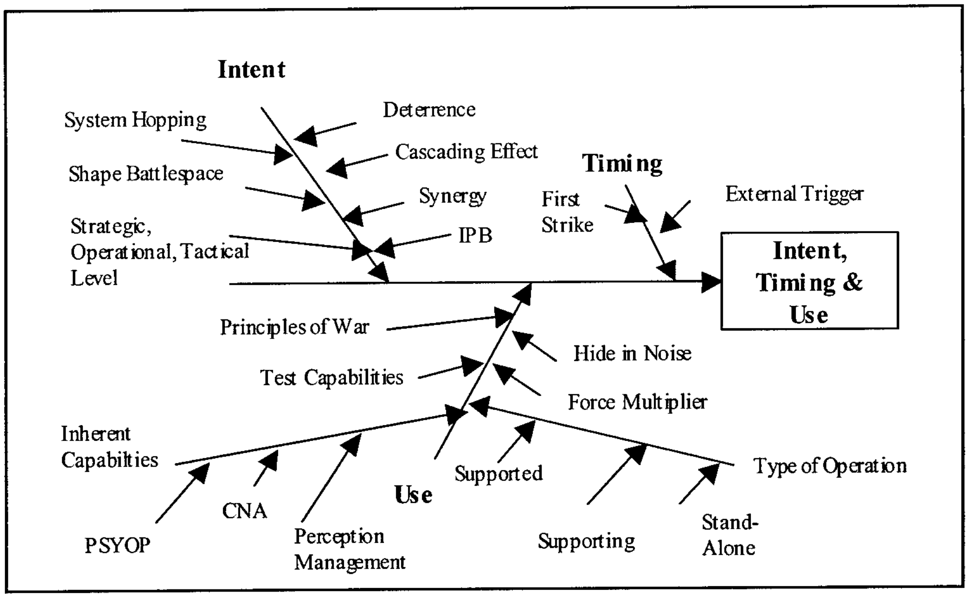


Figure 4-5 Chinese Intent, Timing, and Use of IO

4.3.6. Cultural Impacts

First, as noted previously, the Chinese tend to think with a longer view than their Western counterparts (Thomas: 17). Immediate gain is weighed against potential gain over the next several generations. This might be seen as the perfect mindset to adopt a "low and slow" attack approach for collecting intelligence on US systems. In this case, the risk of not noticing the attacks in the normal network traffic, or inadvertently mistaking the efforts for those of script kiddies, may be greater.

This could also represent an aspect of national personality for the Chinese, as would the Chinese focus on their own history, military philosophy, and military art separate from influence by other's concepts (Thomas: 1). This does not mean that the Chinese ignore potential benefits to be found in the ideas of other nations, but that the emphasis always seems to return to adaptation of foreign ideas to the Chinese viewpoint (Chinese characteristics) (Thomas: 1; Farris, 2000: 70).

An additional form of national personality may be the Chinese viewpoint that it will often be the weaker power being attacked by stronger nations (Thomas: 2; Farris, 2000: 76). This viewpoint has influenced how China focuses its IW efforts.

While the researcher does not have enough knowledge of Chinese culture to truly tailor this factor to the Chinese, those issues addressed in the references will be discussed.

Nationalism and Patriotism

The Chinese appear to a well-developed sense of national identity and patriotism. The large size of the PLA, and the history of waging "People's War" on invading enemies would support this view (Thomas: 2-3).

This concept also appears with respect to how China views violations of its sovereign cyberspace. Thomas believes that violations of cyberspace are considered more important than traditional violations of national sovereignty due to the secretive nature of the Chinese civilian and military information infrastructures (Thomas: 5).

Paradigms and Perspectives

The Chinese have exhibited great care in developing views and doctrine with respect to IW that uniquely reflect the Chinese culture (Thomas: 1). Perception management plays a large role in both civilian and military life (Farris, 2000: 70). This extends to computer network monitoring of Chinese Internet traffic to detect and control traitorous comments (Farris: 2000: 28-29). According to Farris, the US views perception management primarily from a military standpoint (Farris, 2000: 70).

A final aspect of paradigms that US analysts should consider is the caution, put forth by Farris, that Chinese articles and studies may be “merely discussing US concepts without applying them to China” (Farris, 2000: 9). Since publications by Chinese military members, leaders, and scholars serve as one of the primary data sources for understanding Chinese culture, politics, and military objectives and capabilities, one would do well to heed Farris’ warning.

Religion

Religion does not appear to have played a large role in the political or military structure of China as of the date of the references used to build this case study. More recently, the Chinese government has been responding to a perceived threat from the Falun Gong religious sect. In this case, the Chinese government is not acting in line with an existing national religious culture, which is the original intent of this aspect of the framework. However, their response is toward a religious movement, and therefore should be considered.

The Chinese government vowed to eliminate the practice of Falun Gong, labeled an “evil cult”, in 1999 (Dorgan, 2000). More recently, the Chinese government has pronounced the sect to be a reactionary political group aimed at change of China’s socialist system (Dorgan, 2000). Both sides are using the Internet in an attempt to garner support among the Chinese people and the world at large (Dorgan, 2000).

One could also explore how Maoism and Marxism, as belief systems, might provide a similar impact on the Chinese culture as other beliefs systems more directly perceived as being “religious”.

Cyberculture

The use of computer network monitoring by government officials may serve to limit the development of cyberculture in China (Farris, 2000: 28-29). However, one may choose to interpret the large scale efforts of Chinese hackers in attacking US civilian, military, and government websites following the accidental bombing of the Chinese Embassy in Kosovo (Thomas: 12). Recent modernization plans for China include efforts to expand both the military and civilian information infrastructures, which may facilitate further development of Chinese hacker culture, and provide Chinese hackers with increased access to other hackers world-wide (Farris, 2000: 8; Thomas: 17)

Morality

There is an insufficient level of detail in the open source references to address issues of morality with respect to Chinese hackers.

Legality

Aspects of legality were only addressed in terms of instruction in rules and regulations pertaining to IW (Thomas: 10). None of the references provided input on how the Chinese view human life, although US concerns over past human rights violations may cast this detail in an unfavorable light with respect to the Chinese.

Psychological Theory

There is insufficient level of detail in the open source reference documents to address specific aspects of psychological theory as it applies to Chinese hackers. Expert judgment is needed to choose among and utilize the available psychological theories with respect to a specific set of information and situations. Additionally, aspects of culture will need to be considered.

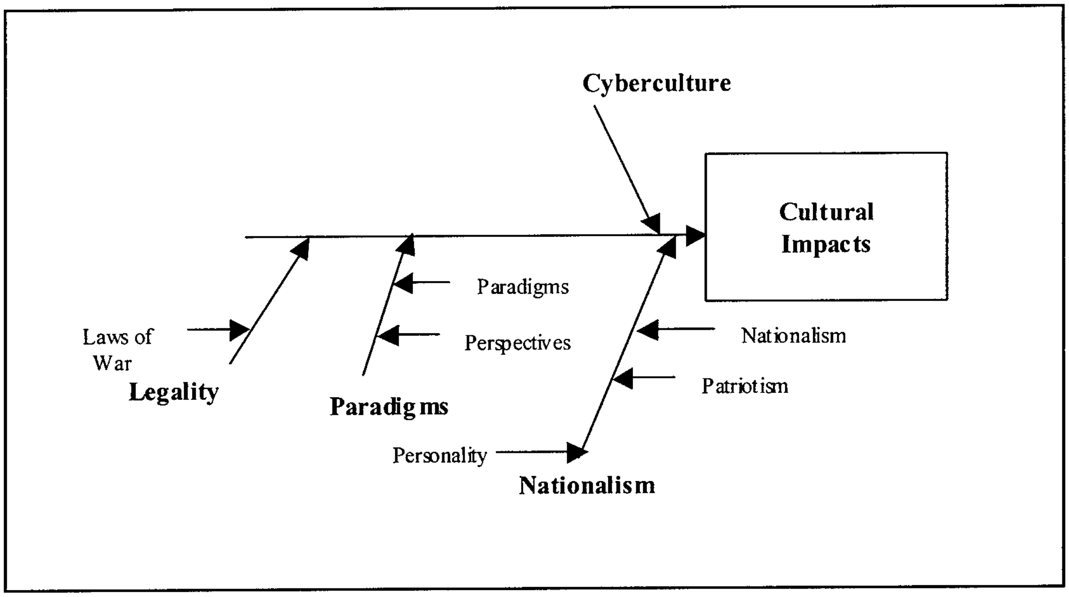


Figure 4-6 Chinese Cultural Impacts

4.3.7. Leadership, Doctrine, and Policy

The Chinese have spent some effort on developing concepts of leadership, doctrine and policy since the emergence of IW. Examples include the extension of the concept of the People's War to IW and the concept of a separate "net force" on par with land, air, and sea forces (Thomas: 1).

Leadership

The existing high-level military leadership is in a similar position to that of the US. New skills must be developed, and the concepts of IW as a fully functioning method of warfare must be internalized. Several levels of IW training have already been established, but Thomas currently considers the IW expertise and "culture" of Chinese leaders to be relatively low (Thomas: 9-11). Several sources noted that Chinese leadership has spent significant time in studying both the Gulf War (often considered the first "modern technology" war) and air operations over Kosovo (Farris, 2000: 7; Thomas: 12). However, Chinese leadership are held as having little practical experience in IW using high technology (Farris, 2000: 7). As such, their "comfort level" with IW and understanding of IW strengths and weaknesses may limit their use of these new capabilities. Leaders may prefer to depend upon more conventional weapons systems and operational plans rather than risk that the results of an IW operation were less than expected. The situation would be similar that of airpower before air doctrine was developed and the Air Force established.

Finally, Senior Colonel Wang Baocun and Li Fei suggest that future Chinese military officer corps will consist more of highly skilled, technical specialists and less of the traditional staff and command billets. They predict that the overall number of units, as well as unit size, will decrease. The units themselves will become more multifunctional and better integrated (Pillsbury, 2001).

Organizational Structure

Potentially one of the greatest aspects of organizational structure on the Chinese approach to IW is the suggestion of a separate "net force" specifically address IW (Thomas: 1; Pillsbury, 2001).

Current Chinese writings also suggest a focus on overcoming the weaknesses of large, non-automated command structures (Farris, 2000:8). Chiang Mengxiong, a Chinese IW scholar, specifically addressed organizational structure when writing on weapons of the 21st century. He supports moving to more networked structures, allowing centralized command at high levels, reduction in middle levels of command, and enabling independent command at the lower levels (Pillsbury, 2001). Military and civilian information infrastructures must be further developed in order to support this goal (Thomas: 17). China's goal is to allow greater flexibility for lower level commanders in adjusting to changes in local conditions, while providing them with sufficient information to ensure that the overall plans of higher headquarters are supported (Pillsbury, 2001). This would represent a mixed organizational structure – neither strictly hierarchical nor strictly networked. It is interesting that Berger suggests a similar structure for the US military (Berger, 1998:

Doctrine and Policy

In China's case, Major General Wang Pufeng believes that IW will emerge as a new theory of war, but he also states that Marxist and Maoist theory must be considered as well (Pillsbury, 2001). In this light, Chinese doctrine will more closely resemble Russian approaches to IW than those of the Western nations (Thomas: 1). Major General Wang Pufeng also states that changes to existing doctrine, strategy, and tactics are vital to the success of IW and the information revolution (Pillsbury, 2001). Additionally, the Chinese tendency to take a long-view with respect to strategic concepts and thought processes must be considered (Thomas: 17). Rather than meeting an adversary at the nation's border, traditional doctrine of the People's War involves absorbing enemy forces into the interior of the country, where Chinese strengths in numbers and geographic knowledge can be brought to bear. Doctrine for IW has been developed with this same thought in mind (Thomas: 1). Chinese secrecy with regards to national information infrastructures, and how violations of cyberspace are viewed, contribute to this concept (Thomas: 5).

Additionally, Chinese doctrine for an information warfare based People's War still includes the concept of the "people", not just active duty military, participating in conflicts – the idea of a "take home battle" (Thomas: 3). Traditionally, China has postured itself and its doctrine as a weaker nation beset by stronger enemies (Farris, 2000: 76).

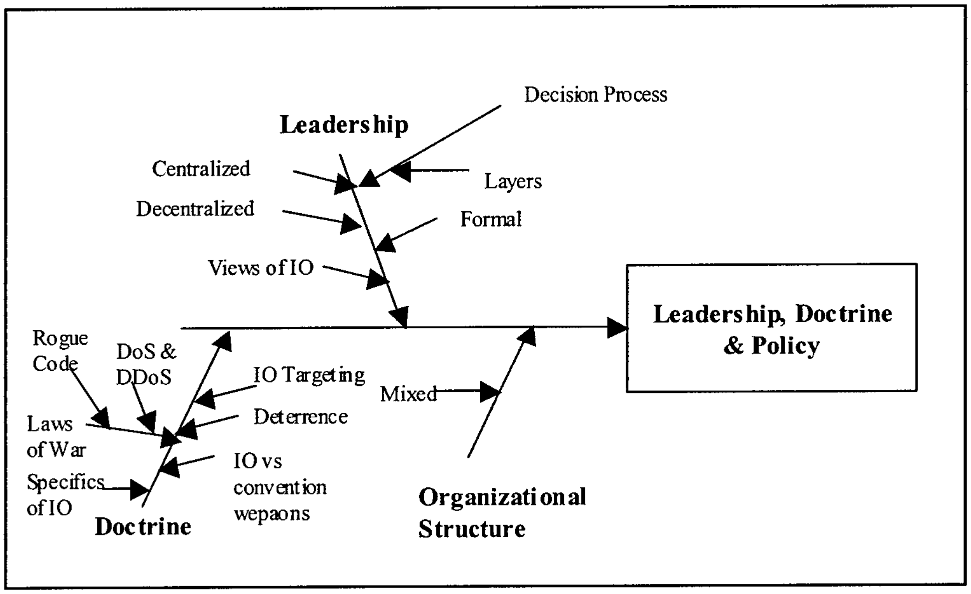


Figure 4-7 Chinese Leadership, Doctrine and Policy

4.4. Chinese Framework for Malicious Hacking

The knowledge gained exploring each of the key aspects of malicious hacking with respect to the Chinese is now consolidated into the proposed framework. This allows for insight into strengths and approaches to IO and IW that can improve threat warnings and assessments, as well as contribute to more rapid and / or automated attack responses to perceived efforts at collecting against or targeting US information and information systems.

One of the key insights from this analysis is the cultural difference in approaches to IW. The tools and techniques remain the same, but the level at which IO and IW is incorporated into both the civilian and military aspects of society differ. The People's War concept, with the possibility of "take home battle" against the US via laptops sending rogue code and DoS or DDoS attacks over communications systems worldwide is sobering. Recent events in the Middle East support the concept of everyday citizens participating in IW (Associated Press, 2000; Gentile, 2000).

Efforts to profile state sanctioned hackers would capture aspects of this form of warfare through detailing the nation's culture, intent, doctrine, and individual skill levels.

Figure 4-8 Chinese Malicious Hacker Profile provides the overall framework tailored to open source, published summaries of Chinese doctrine and views of IW.

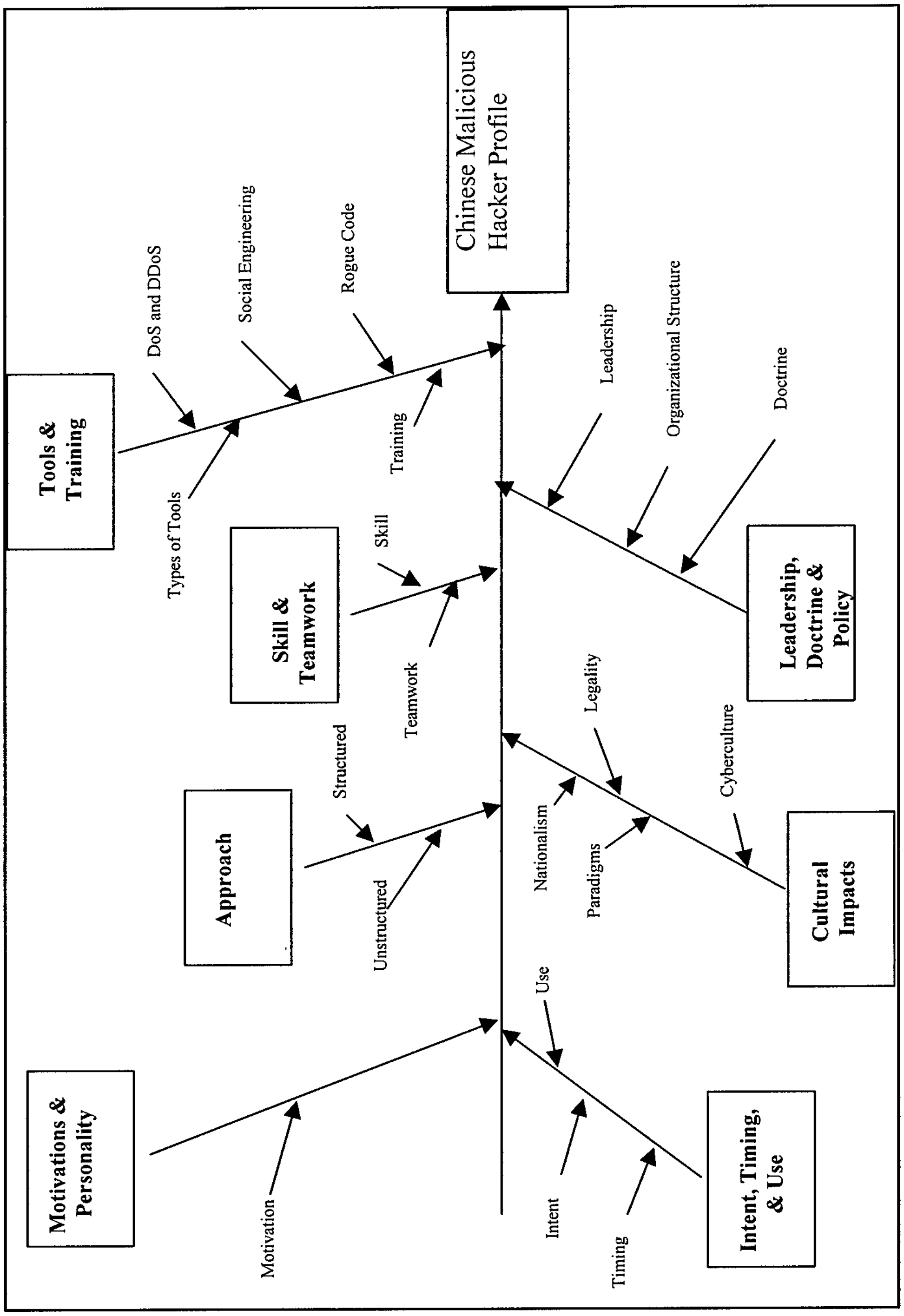


Figure 4-8 Chinese Malicious Hacker Profile

4.5. Conclusions

The case study provides a sound example of how the malicious hacker profile developed in Chapter Three can be applied to foreign IO and IW programs. A limitation of the case study is the author's lack of background in Chinese culture and military history, as well as the restriction to open source information. However, the open source references utilized to tailor the basic framework to Chinese IO units are sufficient to illustrate the framework's applicability.

Of particular interest is the Chinese concept of the People's War. This provides a large body of both high and low levels of expertise that can be called upon in times of conflict to launch attacks simultaneously and over sustained periods of time. The large Chinese population, if motivated to participate even in part in a DoS, DDoS, or virus launching attack, could have a strong impact on the outcome of a future conflict. More efforts should be spent in evaluating the impact of this concept on US computer defenses at all levels of information infrastructure.

The high levels of patriotism and military involvement in the Chinese culture also strongly color their approach to IO. Cases such as the accidental US bombing of the Chinese Embassy in Kosovo highlight potential external triggers of Chinese (and other nation's) hacking. The Chinese long-term view of strategy and success, and admission of intelligence collection efforts, would also lead one to explore low-level IPB efforts.

In conclusion, the fishbone diagram provides a sound and visually elegant method of consolidating intelligence products and information on foreign IO organizations and analyzing their strengths, weaknesses, and influence points. To prove effective over time, this framework must be updated as Chinese (or other nation's) IO and IW theory, practice, and expertise evolve.

5. Findings and Conclusions

5.1. Overview

This thesis has presented a comprehensive overview of malicious hackers and the world in which they operate. A framework has been presented that organizes key aspects about hackers into a model that can be analyzed.

The results of the effort include a framework for analyzing individual hackers, or average members of IO cells, from the category of nation state actors. Additionally, this framework can be used as a basis for analysis of malicious hackers belonging to transnational terrorist or criminal organizations.

A case study was developed and presented to illustrate the uses of the framework that is proposed. China was chosen as the nation of interest for the case study due to its early interest in IO and IW concepts and programs, and due to open source documentation on Chinese views on IO, doctrine, and military efforts in the development of IO capabilities.

5.2. Objectives of Study

Throughout this effort, the underlying desire was to move forward the current state of profiling with respect to malicious hackers. With a recognized need for improved Threat Warning and Assessment in the realm of Information Operations, a framework was presented that allows those combating malicious hackers to better understand and respond to their adversaries.

5.3. Limitations

One key limitation of this effort was the availability of data, and the restriction to open source information. Without data from past, substantiated attacks, whether from individuals acting outside the framework of an organized structure or from those acting on behalf of recognized, structured threats, this effort relied upon past analysis of hackers and published doctrine for US IO efforts.

An additional limitation was access to expertise in the fields of computer security, threat warning and analysis, and profiling. This contributed in the effort remaining at the unclassified level, with "data" for the framework developed being open source. This is not to say that the results are not valid. Rather, it acknowledges the fact that expertise and intelligence sources exist that can improve the level of detail in any profiles that are developed as a result of this effort. For this reason, results of the framework developed should be considered indicative of an "average" member of an IO group for the nation being evaluated, and not predictive of any specific member.

Finally, it must be remembered that a specific profile is only as useful as it is up-to-date. Technology, unit capabilities, skill levels, tools, and doctrine are changing rapidly in the information age. To be effective, a nation's hacker profile must change as well.

5.4. Recommendations for Further Study

Computer technology is advancing at a pace that makes it extremely difficult, if not impossible, to understand and synthesize. As discussed in Chapter Three, hackers have the advantage of time and specialization when it comes to knowing the "ins and outs" of any given aspect of computer technology. While a hacker can specialize in specific operating systems and hardware platforms, a computer systems administrator must, due to organizational needs, become a "jack of all trades" with rudimentary to moderate knowledge of a wealth of computer systems. This makes the system administrator's role often one of reaction to past or ongoing attacks. The number of hacker tools available on the Internet grows every day, allowing anyone with a computer and a modem the chance to become a hacker. Knowing the enemy – motivations, true intent, and even their identity – will rarely be the same in cyberspace as in the physical world of previous wars. For these reasons, and many others, the work begun by this thesis and all of its predecessors, is just the tip of the proverbial iceberg.

Several areas with the potential for large rewards were identified during the course of this thesis. A first effort would involve statistical analysis of substantiated incidents, as discussed in Chapter Two. Additional details with regard to hacker types, skills, tools, approaches, and aspects of teamwork might be identified by such an effort. The results of such analysis would provide several benefits. Aspects of the model developed in this effort could be validated by real world attacks from nations of interest, and additional aspects of the model that can be substantiated by the data might be developed. Data analysis would also assist in automated response to attacks, once characteristics of the attacks can be tied to types of hackers or the intent behind their actions.

Second, the framework presented in this thesis could be expanded for additional types of threats. The differences that exist between foreign actors and national actors, insiders, script kiddies, and political dissidents of all varieties could be explored.

Additionally, using the Value of Information hierarchy from Hamill's thesis and various efforts in risk-based approaches to system protection, a new perspective in analyzing computer assurance could be developed that would allow for clear trade-offs between capability of the computer system, analyzed threats and vulnerabilities, and the value of the information being protected (Hamill, 2000). Finally, a value model of malicious hackers could be built, using members of various Red Teams as the decision makers. In this case, a VFT approach would provide hierarchy of what is important to hackers in breaking into a system. An effort could be made to separate those aspects of the values and objectives into those common to all hackers, cultural elements important to a specific group of hackers, and those values of the individual hackers themselves as opposed to the groups in which they operate. Renfro's past work in profiling individuals would prove a valuable starting point (Renfro, 2000).

Future work would extend this model to more types of hackers, and further detail the hacker profile model. There is a recognized need to update the models developed as the group's profiles react to world changes. An additional area of particular interest to many in the DoD would be profiling of potential "insider" attackers, as well as ways to see a small, sustained attack that is hiding in the "white noise" of normal system traffic or "script kiddy" type probes. In addition, future research could focus on automated ways to tie multiple distributed attacks together and to the underlying attacker. A predictive model of hacker behavior could also be developed once the descriptive model has proved operationally sound.

A more near term research extension would be tying the types of attacks a particular type of hacker is more prone to use. Hackers reacting to different motivations would be pursuing different goals – such as information mining, denial of service, corruption or deletion of data. Based upon the profiles developed for different hackers and the signatures of attacks, anticipation of attacks and directed responses can be developed.

5.5. Conclusions

In summary, a framework has been developed that draws upon the strengths of past efforts in hacker profiling, but that specifically focuses on structured attacks from hackers employed by foreign governments. The basic framework needs to be tailored to each nation of interest, with specific expertise in that nation's culture, doctrine, and military structure utilized in the analysis.

More work remains in this area, as doctrine, capabilities, and structure of IO groups will change with the technology. Further efforts in profiling potential adversaries will only improve the ability of US forces to respond to IO and IW threats regardless of their point of origin.

Bibliography

Ackerman, Gwen, "'Analyzer' enlisted to defend Israeli sites against Web violence," The Jerusalem Post, November 16 2000.

African Business. "Soldier of Fortune – the mercenary as corporate executive," December 1997.

Aldrich, Richard W. "Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Regime," INSS Occasional Paper 32, Information Operations Series: ix – 92 (April 2000).

Anonymous. Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network (2nd Edition). Indianapolis IN: SAMS Publishing, 1998.

Arkes, Hal R. and John P. Garske. Psychological Theories of Motivation (2nd Edition). Monterey CA: Brooks / Cole Publishing Company, 1982.

Associated Press. "Crackers Attack Pro-Israeli Site," WiredNews. November 3 2000.

Barbera, Salvador, Peter J. Hammond, and Christian Siedl, editors. Handbook of Utility Theory. Norwell MA: Kluwer Academic Publications, 1998.

Berger, Alexander. Organizational Innovation and Redesign in the Information Age: The Drug War, Netwar, and Other Low-End Conflict. Department of National Security Affairs, Naval Postgraduate School, Monterey CA, March 1998.

Boldrick, Michael R. "Information Warfare: The Next Major Challenge in Military Strategies and Operational Planning," Soldier-Scholar: 11–19 (Fall 1996).

Borland, John. "Governments Beat Terrorists to Net Weapons," TechWeb News. article released 22 September 1998. http://www.techweb.com/wire/story/TWB19980922S0018. 25 July 2000.

Chantler, Nicholas. Risk: The Profile of the Computer Hacker. Ph.D. dissertation, Curtin University of Technology, Perth, Western Australia, March 1996.

Computer Emergency Response Team/Coordination Center (CERT/CC). CERT/CC Statistics: 1988 – 2000. Pittsburgh: Carnegie Mellon Software Engineering Institute, http://www.cert.org/stats/cert_stat.html. 9 February 2001.

Computer Security Institute. "CSI/FBI 1999 Computer Crime and Security Survey". CSI report. http://www.gocsi.com/losses.htm. 24 August 2000.

Cooley, William W. and Paul R. Lohnes. Multivariate Data Analysis. New York NY: John Wiley & Sons, Inc., 1971.

Costin, Harry. Readings in Total Quality Management. Fort Worth TX: Harcourt Brace and Company, 1994.

Curphy, Gordon J., Richard L. Hughes, and Robert C. Ginnett. Leadership. Homewood: Irwin, 1993.

Denning, Dorothy E. Information Warfare and Security. Reading MA: Addison Wesley Longman, Inc., 1999.

Department of Defense, Joint Chiefs of Staff. Joint Publication 3-13, Joint Doctrine for Information Operations. Washington: Pentagon, 9 Oct 1998.

Department of Defense, Office of the General Counsel. An Assessment of International Legal Issues in Information Operations. Washington: Pentagon, May 1999.

Department of the Air Force. Air Force Basic Doctrine. AFDD 1. Washington: HQ USAF, September 1997.

Department of the Air Force. Nuclear Operations. AFDD 2-1.5. Washington: HQ USAF, 15 July 1998.

Department of the Air Force. Information Operations. AFDD 2-5. Washington: HQ USAF, 5 August 1998.

Dorgan, Michael. "China casts banned sect as political subversion," San Jose Mercury News. article released 21 October 2000. http://www.CENSUR.com.
27 February 2001.

Edwards, Harry. "Hacker Exposes Computer Security Benefits," AirForceNews. article released 14 July 2000. http//www.af.mil/news/Jul2000/n20000713_001064.html.
18 July 2000.

Falmagne, J.-Cl. "Stochastic Token Theory," Journal of Mathematical Psychology 41: 129 – 143 (1997).

Farris, Kate. "Chinese Views on Information Warfare." Unpublished report, 2 April 2000.

"Fight-Back! Against Hackers." Unpublished report. http://www.antionline.com/fight-back/. 25 Jul 2000.

Fogleman, Ronald R., USAF Chief of Staff. "Fundamentals of Information Warfare – An Airman's View." Address to the National Security Industry Association – National Defense University Foundation Conference on The Global Information Explosion. Washington DC. 16 May 1995.

Gentile, Carmen J. "Israeli Hackers Vow to Defend," WiredNews. November 15 2000.

Gertz, Bill. "Chinese Espionage Handbook Details Ease of Swiping Secrets," *The Washington Times*. 26 December 2000.

Godwin, Grover M. Hunting Serial Predators: a Multivariate Classification Approach to Profiling Violent Behavior. Boca Raton FL: CRC Press Inc., 2000.

Grier, Peter. "Information Warfare," AIR FORCE Magazine: 34 – 37 (March 1995).

Hair, Joseph F., Rolph E. Anderson, Ronald L. Tatham, and William C. Black. Multivariate Data Analysis with Readings. (3rd edition) New York NY: Macmillan Publishing Company, 1992.

Hamill, J. Todd. Modeling Information Assurance: A Value Focused Thinking Approach. MS Thesis, AFIT/GOR/ENS/00M-15. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2000.

Hoffman, David. "Russian Touts Computer Virus as Weapon," Washington Post. 9 May 2000.

Huang, J. H., translator. Sun Tzu The Art of War: The New Translation. New York NY: Quill William Morrow, 1993.

Hulin, Charles L., Fritz Drasgow, and Charles K. Parsons. Item Response Theory: Application to Psychological Measurement. Homewood IL: Dow-Jones Irwin, 1983.

Islam, Towhidul, Jordan Louviere, and Robert Bartels. "An Empirical Analysis of Household Level New Product Trial and Repeat Data." Paper presented to RU2000, Duke University, August 2000.

Jackson, Janet L., and Debra A. Bekerian. Offender Profiling: Theory, Research, and Practice. New York NY: Wiley Press, 1997.

Kerchner, Philip M. Jr. Value-Focused Thinking Approach to Psychological Operations. MS Thesis, AFIT/GOR/ENS/99M-07. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 1999.

Kiras, James. "Information Warfare and the Face of Conflict in the Twenty-First Century," Soldier-Scholar: 40 – 42 (Fall 1996).

Lavadour, Justin W. Pitfalls of the A-76 Process. MS Thesis, AFIT/GLM/ENS/01M. School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2001.

Lemon, Dave. AIA contractor. "Threat to Computer Systems & Networks." Briefing to AIA Cyber Summit attendees, Air Intelligence Center, Kelly AFB TX. 15 August 2000.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini. Countering the New Terrorism. Santa Monica: RAND, 1996 (RAND MR-989-AF). http://www.rand.org/publications/MR/MR989/MRM989.pdf. 28 August 2000.

McClure, Stuart, Joel Scambray and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. Berkeley CA: Osborne / McGraw-Hill, 1999.

Machiavelli, Niccolo. The Prince. New York: Oxford University Press, Inc., 1962.

Mardia, K.V., J. T. Kent, and J. M. Bibby. Multivariate Analysis. San Diego CA: Academic Press Limited, 1994.

Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network (2nd edition). Indianapolis IN: SAMS Publishing, 1998.

Maydeu-Olivares, Albert. "Limited Information Estimation and Testing of Thurstonian Models for Preference Data." Paper presented to RU2000, Duke University, August 2000.

Meller, Paul. "Council of Europe to discuss cyber crime treaty," InfoWorld.com. 22 November 2000.

Meyer, Gordon R. The Social Organization of the Computer Underground. MA Thesis. Department of Sociology, Northern Illinois University, Dekalb IL, August 1989.

Minihan, Kenneth A. "Intelligence and Information Systems Security: Partners in Defensive Information Warfare," Defense Intelligence Journal, 5-1: 13–23 (1996).

Mitra, Amitava. Fundamentals of Quality Control and Improvement. New York NY: Macmillan Publishing Company, 1993.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. Strategic Information Warfare: A New Face of War. Santa Monica: RAND, 1996 (RAND MR-661-OSD).

Nahmias, Steven. Production and Operations Analysis (2^{nd} edition). Homewood IL: Irwin, 1993.

Ozeki, Kazuo, and Tetsuichi Asaka. Handbook of Quality Tools: The Japanese Approach. Cambridge MA: Productivity Press, Inc, 1990.

Pagnoni, Anastasia. Project Engineering: Computer-Oriented Planning and Operational Decision Making. New York NY: Springer-Verlag, 1990.

Peterson, James L. Petri Net Theory and the Modeling of Systems. Englewood Cliffs NJ: Prentice-Hall, Inc., 1981.

Pew, Richard W. and Anne S. Mavor, editors. Modeling Human and Organizational Behavior. Washington DC: National Academy Press, 1998.

Renfro, Rob. "Modeling Individual Behavior". Unpublished report for the School of Engineering, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, 2000.

Rouland, Chris. Director X-Force. Briefing to CIA INFOSEC Malicious Code Seminar, Central Intelligence Agency, Washington DC. 29 November 2000.

Scott, William B. "Information Warfare Policies Called Critical to National Security," Aviation Week & Space Technology: 60–64 (28 October 1996).

Smith, Richard. CTO, Privacy Foundation. Briefing to CIA INFOSEC Malicious Code Seminar, Central Intelligence Agency, Washington DC. 29 November 2000.

Stevens, Halbert F. "Information Dominance: The New High Ground," Defense Intelligence Journal, 5-1: 43–52 (1996).

Taylor, Paul A. Hackers: Crime in the Digital Sublime. New York NY: Routledge, 1999.

Thomas, Timothy L. Like Adding Wings to the Tiger: Chinese Information War Theory and Practice. Fort Leavenworth KS: Foreign Military Studies Office, www.fas.org.

Turvey, Brent E. Criminal Profiling: an Introduction to Behavioral Evidence Analysis. San Diego CA: Academic Press, 1999.

Pillsbury, Michael, editor. Chinese Views of Future Warfare, revised edition. http://www.ndu.edu/inss/books/chinview/chinapt4.html 4 January 2001.

Verton, Dan. "NSA warns it can't keep up with rapid changes in IT," Infoworld.com article. http://www.infoworld.com. 21 February 2001.

Vistica, Gregory. "Inside the Secret Cyberwar: Facing Unseen Enemies, the Feds Try to Stay A Step Ahead," Newsweek article. http://newsweek.com/nw-srv/printed/us/st/a16330-2000feb13.htm. 18 Februrary, 2000.

Vranesevich, John. "How to Be a Hacker Profiler." Unpublished special report. http://www.antionline.com/SpecialReports/hacker-profiler/category.html. 24 July 2000.

Weiss, David J., editor. New Horizons in Testing: Latent Trait Test Theory and Computerized Adaptive Testing. New York NY: Academic Press, 1983.

Winchell, William. Continuous Quality Improvement: A Manufacturing Professional's Guide. Dearborn MI: Society of American Engineers, 1991.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 20/03/2001	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From – To)* June 2000 - March 2001

4. TITLE AND SUBTITLE
MALICIOUS HACKERS: A FRAMEWORK FOR ANALYSIS AND CASE STUDY

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
KLEEN, LAURA J. , CAPTAIN, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/ENS)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT/GOR/ENS/01M-09

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
DARPA/ISO/IASET
Attn: Mr. Steve Carroll
3701 North Fairfax Drive
Arlington, Virginia 22203-1714
scarroll@darpa.mil, 703-696-2235

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Recent years have seen an increase in the number and severity of Information Operations (IO) attacks upon DoD resources by individuals and groups seeking thrills, monetary gain, publicity, and myriad other goals. This effort develops a first cut model of individual hacker mentality that can be utilized to improve risk and threat assessments, mitigate Information Assurance (IA) vulnerabilities. Further, it is a first step toward automated characterization of Information Warfare (IW) attacks based upon hacker types.

All hackers are not the same; therefore one must understand who they are to best deal with their actions and the intent behind them. Many hackers are not malicious. However, others are intent upon gathering information for gain, corrupting data, denying access, or to see what harm they can cause. This effort specifically focused on malicious hackers working for nation states. Results include advances in the way that hackers are classified and profiled, with a better understanding of their values, skills, and approaches to hacking. Responses can then be tailored to specifics of a given class of hackers. The model developed is illustrated by a case study.

15. SUBJECT TERMS
Information Operations, Information Surveillance, Motivation +, Statistical Analysis

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Dr. Richard F. Deckro
a. REPORT	b. ABSTRACT	c. THIS PAGE			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U	UU	221	(937) 255-6565, ext 4325/Richard.Deckro@afit.edu